ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2016.0198

AUDIO CRYPTANALYSIS - AN APPLICATION OF SYMMETRIC KEY CRYPTOGRAPHY AND AUDIO STEGANOGRAPHY

Smita Paira[1] and Sourabh Chandra[2]

[1]*Department of Computer Science and Technology, Indian Institute of Engineering Science and Technology, India*
E-mail: [1]smtpaira@gmail.com

[2]*Department of Computer Science and Engineering, Calcutta Institute of Technology, India*
E-mail: [2]sourabh.chandra@gmail.com

Abstract

In the recent trend of network and technology, "Cryptography" and "Steganography" have emerged out as the essential elements of providing network security. Although Cryptography plays a major role in the fabrication and modification of the secret message into an encrypted version yet it has certain drawbacks. Steganography is the art that meets one of the basic limitations of Cryptography. In this paper, a new algorithm has been proposed based on both Symmetric Key Cryptography and Audio Steganography. The combination of a randomly generated Symmetric Key along with LSB technique of Audio Steganography sends a secret message unrecognizable through an insecure medium. The Stego File generated is almost lossless giving a 100 percent recovery of the original message. This paper also presents a detailed experimental analysis of the algorithm with a brief comparison with other existing algorithms and a future scope. The experimental verification and security issues are promising.

Keywords:

Symmetric Key Cryptography, Audio Steganography, LSB Technique, Cover File, Stego File.

1. INTRODUCTION

Cryptography and Steganography are the two techniques that play a vital role in the revolutionized digital world. Cryptography means hidden writing [14] and Steganography means covered writing [2]. As the message travels from one place to another [3], it is prone to many intermediate attacks. Cryptography uses two keys for encryption and decryption namely private key and public key.

- Symmetric Key Cryptography: Single key (Private, Secret and Shared). It is based on Substitution and Permutations of symbols [4], [5].
- Asymmetric Key Cryptography: Two keys (Public Key for encryption and Private Key for decryption). Requires a highly secure channel [6] and consumes much power [7].

Features provided by Cryptography are confidentiality, integrity, authenticity and non- repudiation. The conventional methods of Cryptography are AES, DES, 3DES, RSA, Diffie-Hellman, Blowfish, ECC, Digital Signatures, etc [1].

Although Cryptography encrypts a message to an unrecognized version (alteration of structure [18]), it creates suspicion in hacker's mind to break the key to find out the encrypted original data. To solve this problem Steganography is used. In this technique, the secret is covered by a digital data. The digital data may be an image, audio or video depending upon the nessecity and security. By seeing the digital data one cannot even aware of the hidden information concealed behind the Covered Medium [9], [17]. The various Audio Steganography methods are LSB Coding, Echo Hiding, Parity Coding, Phase Coding, Spread Spectrum, etc [15].

In this paper, a new algorithm has been proposed. This is an application of both Symmetric Key Cryptography and Steganography. The application both the security techniques increases the security of the secret shared data with a high degree of confidentiality and integrity. The Cryptographic algorithm used consists of a randomly generated key with simple indexing and addition techniques and the Steganography algorithm used is the LSB technique. In this method, the Covered Medium used is an Audio File. During transmission, there is a huge probability of the damage of the Audio Header [13]. The default Header size of an Audio File (.mp3) is usually 4 bytes [19]. For this reason, the aforesaid algorithm works on the body of the Audio File (leaving the first 4 bytes) instead of the Header.

The proposed algorithm has been experimentally tested and verified. The Stego File generated after embedding remains almost lossless, which in turn gives added security to the secret information. The hidden message can only be uncovered by the intended person for whom it is being sent and the data recovery 100 percent. The various steps used in this algorithm along with the experimental analysis and comparative study have been presented in later parts of the paper.

In this algorithm we have used both the concept of Cryptography and Steganography in order to make the algorithm more secure and efficient. Usually after applying the crypto encryption algorithm, the message becomes scrambled and has a huge tendency to bring suspicion in people's mind. The hacker can easily understand that something being hidden. In order to remove such problem we hide the encrypted plain text in an Audio File using LSB Technique. The message remains secure aware of the hacker. Even if the hacker gets the Audio File, the retrieval process is also tough. He has to first extract the Cipher text file and then apply the decryption algorithm. Thus the entire message as well as communication system remains unaffected and secure.

2. UNDERLYING ALGORITHM

2.1 ENCRYPTION OF ORIGINAL PLAIN TEXT FILE USING SYMMETRIC KEY CRYPTO-GRAPHY

Step 1: Read the text file.

Step 2: Find the length of the message.

Step 3: Fetch each character along with its index and follow Step 4 - Step 6

Step 4: Consider any one digit key, say 3

Step 5: Find (Index MOD 3)

Step 6: Add the result from Step 5 to the ASCII of the corresponding character.

2.2 CIPHER KEY GENERATION AND STORAGE

Step 1: Find the last encrypted character and its index.

Step 2: Add the character's ASCII with the sum of its index and key (here, it is 3).

Step 3: Append the new character at the end of the ciphered message.

2.3 GENERATION OF STEGO FILE

Step 1: Read the Ciphered text file.

Step 2: Fetch each characters and store their LSBs in an array.

Step 3: Store the LSBs of individual digits of the original message length in another array.

Step 4: Read the Audio File, to be used as Cover medium.

Step 5: Embed the LSB of the first encrypted character in the LSB of the first Byte of the Audio File, leaving the header.

Step 6: Embed the length LSBs in the remaining 5 Bytes of the Cover File succeeding the first Byte in Step 5.

Step 7: Embed the remaining encrypted characters' LSBs in the 7^{th} Byte of the Cover File onwards using LSB encoding technique following Step 6.

Step 8: Send the Stego File over the communication channel.

2.4 EXTRACTION OF THE CIPHERED MESSAGE FROM THE STEGO FILE

Step 1: Read the Stego File.

Step 2: Using LSB technique, find out the length of the original text file. Apply this technique on 2^{nd} to 6^{th} Bytes leaving the four Header Bytes and first Byte of the Audio Body.

Step 3: Again apply LSB technique on the first byte and 7^{th} Bytes onwards of the Body the Stego File, leaving the header. Apply this technique until the length of the message found in Step 2.

Step 4: Store the message obtained from Step 3 in a file.

2.5 DECRYPTION OF CIPHERED KEY

Step 1: Read the partially decrypted text file.

Step 2: Find the index of the last character.

Step 3: Find (Index MOD 3)

Step 4: Find the ASCIIs of last and last second characters.

Step 5: Add the ASCII of the last second character with the result obtained from Step 3.

Step 6: Subtract the result obtained in Step 5 from the ASCII value of the last character.

2.6 DECRYPTION OF THE MESSAGE USING SYMMETRIC KEY CRYPTOGRAPHY

Step 1: Read the partially decrypted text file.

Step 2: Fetch each character and its index up to the last second index and follow Step 3-Step

Step 3: Find (Index MOD key)

Step 4: Subtract the result from Step 3 from the ASCII of the corresponding character.

Step 5: Store the decrypted message in a new file.

Step 6: End.

3. PICTORIAL REPRESENTATION OF THE PROPOSED ALGORITHM

The proposed algorithm works on two phases. Initially, the message is encrypted with a Symmetric Key Cryptography algorithm. After that, using suitable LSB technique, the encrypted message is concealed behind an Audio File. The flow of algorithm is shown in Fig.1.

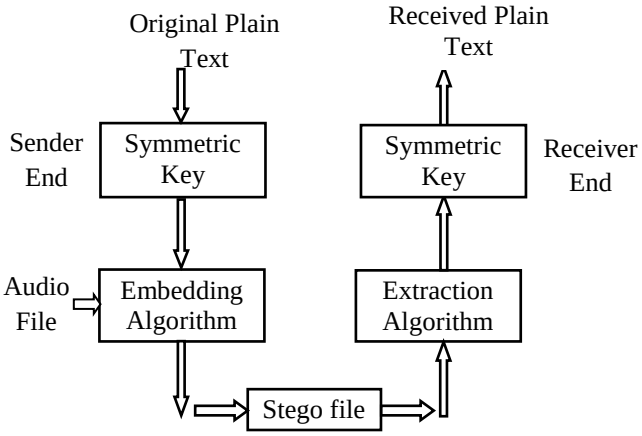


Fig.1. Flow diagram of the proposed algorithm

Let us consider the original message file as shown in Fig.2.

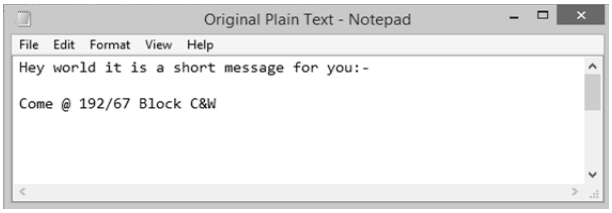


Fig.2. Original Plain Text File

At first, the length of the file is calculated to be 64. Now, the message is encrypted using a random key generated (Symmetric Key). Simple addition and indexing operations have been used in the encryption algorithm. Further the encrypted message is hidden behind the Audio File chosen using LSB technique. The header part of the Audio File remains unaffected. Leaving the header part, the first byte is encoded with the first character of the encrypted message. Succeeding five bytes are reserved for encoding the message size. The remaining bytes of the Cover File are encoded with the remaining characters of the encrypted message. The entire process has been illustrated in Fig.3.

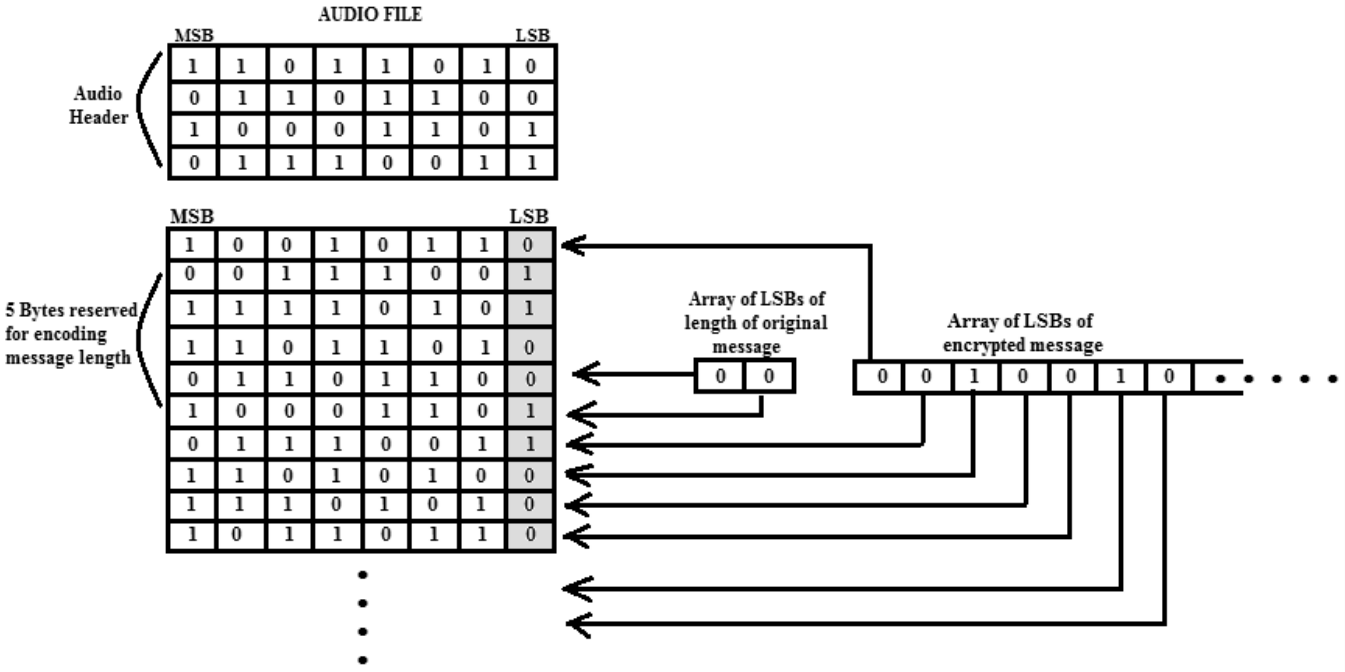


Fig.3. Working principle of the proposed Steganography algorithm

The said algorithm has been implemented on JAVA Eclipse Mars platform. The JAVA interfaces, designed are explained below. There are total four window starting with the main window which contains the three buttons namely EMBED, EXTRACT and EXIT buttons, which moves the control to the respective windows once pressed. The next window is the EXIT window. It wants one to decide whether to exit from the system. If yes, then exits otherwise moves the control back to the main window. The two windows are shown in Fig.4.

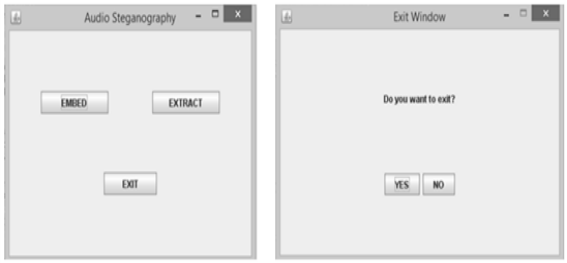


Fig.4. Audio Steganography and Exit Windows

The next window is the EMBED window which selects the Cover File, Message File and the destination to store the Stego File. Then, press the EMBED AND SEND button to encrypt and send the Stego File. The fourth window is the EXTRACT window which selects the Stego File and the place to save the received message after decryption. Then, press the EXTRACT AND SAVE button to extract the message and save it in a file. The Embed and Extract windows work at sender and receiver end respectively and are shown in Fig.5 and Fig.6 respectively.

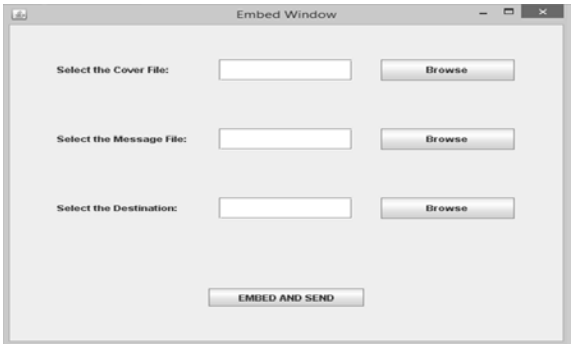


Fig.5. Embed Window

Fig.6. Extract Window

There is a 100 percent recovery of the original message and the received file is shown in Fig.7.

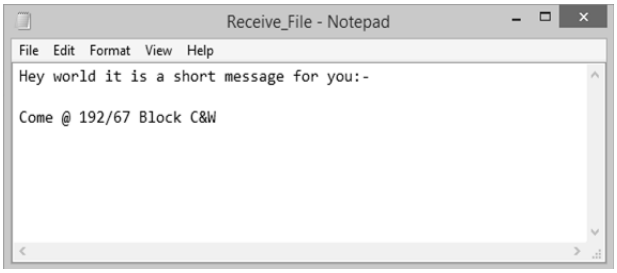


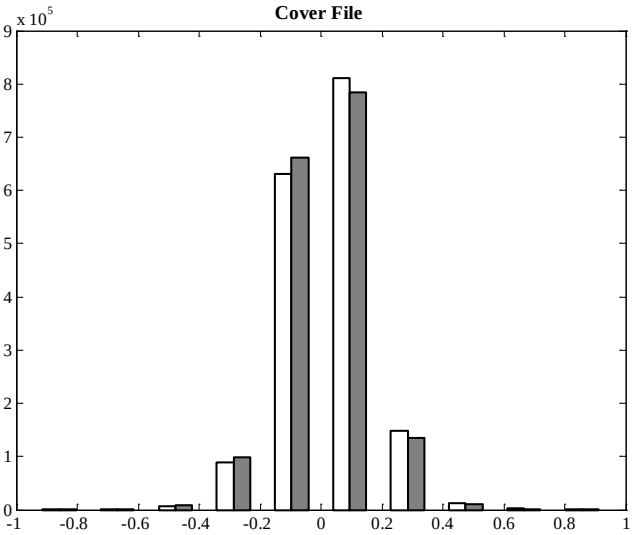
Fig.7. Receive Text File

4. EXPERIMENTAL ANALYSIS OF THE PROPOSED ALGORITHM

In this algorithm, the message is first encrypted using Symmetric Key Cryptography and the encrypted message is embed behind a Cover File. The Stego File obtained is compared with the original Cover File on MATLAB Platform as follows:-

Step 1: Read the two files.

Step 2: Compare the histograms of the two files as shown in Fig.8.



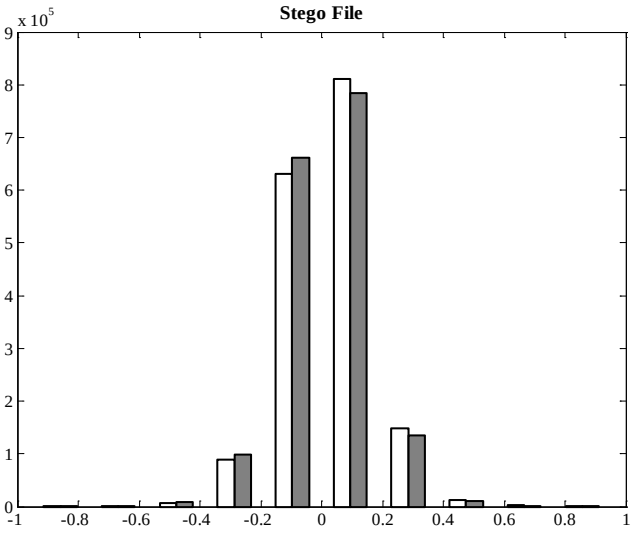


Fig.8. Histogram analysis of Cover File and Stego File

From the above two histograms, it is found that the histograms are almost the same. This means that the Stego File obtained after encoding, remains almost lossless. The targeted LSBs depend on the length of the text file to be embedded and the recovery is 100%. Since, the file after encoding remains almost noiseless, it becomes very difficult to recognize the presence of any concealed message.

Step 3: Calculate the entropies of the two audio files. It is found to be 4.4048 for both the audio files.

Step 4: Calculate the correlation coefficient of the two audio files. It is found to be 1 which means that the two file are almost equal.

The entire process depends on the length of the original text file since only those numbers of bytes are changed. Again, since only LSBs are encoded, the loss is almost negligible.

Table.1. Comparison table of various Symmetric Key Cryptography and Audio Steganography algorithms

METHOD	FEATURES	PROS	CONS
Intelligent Processing [8]	Uses a combination of cryptography and Steganography. Uses a combination of LSB technique with XOR method.	Combination of LSB with XORing method increases the security.	Direct extraction of LSBs only results in noise if XORing method is only used for embedding.
Audio Steganography with Dual Randomness LSB method [9]	It is based on Dual Randomness LSB method. It hides the message in random selected samples, in random selected bits. It uses RSA for encryption and decryption.	Provides better confidentiality than the conventional LSB technique.	Use of Huffman coding increases the capacity of multiple bits.
Variable higher bit approach of Audio Steganography [10]	It uses either of the two consecutive higher bits to hide data. The whole byte is modified with the nearest original Byte value.	As the method does not work on LSB, it is possible to hide additional data bit if needed. Not limited to audio files.	Since, LSBs are ignored it has a relatively lower hiding capacity.
Rotation Based	It uses bit wise circular shift operations for	Use of ciphered key with separate	Once intercepted can be easily

Symmetric key algorithm [7]	encryption and decryption.	space encryption makes the information secure.	hacked.
Trusted third party key indexing method [11]	LSB bit replacement depends on the primary key provided by the Trusted Third party. The secondary key generated during embedding process, is communicated to the decoder end.	The two keys along with the message retrieval code increases the security of the data.	Best suited for 32 bit audio files with an availability of more LSBs.
LSB based Audio Steganography for hiding secret information [12]	Embeds text information in an audio file using LSB technique. The performance of the algorithm is calculated using SNR values of the inputted audio.	Increases the capacity of the stego system.	No such drawback but the security can be increased by adding cryptographic algorithms.
Symmetric key encryption through binary-gray conversion and data structures [5]	Application of data structures with binary-gray conversion for encryption and decryption.	Linked ciphered key with space encryption increases the confidentiality of the data.	Complexity depends on the size of the message.
Enhanced LSB Technique for audio Steganography [13]	Sampling of the audio file followed by modifications at least significant bits.	Does not have any effect on the size of the audio file.	Use of bits other than the LSBs after sampling may cause noise.
Detection of LSB Steganography using Sample Pair analysis [16]	It is used to detect the LSB Steganography in digital images and audios. Length of the information can be calculated with a relatively high precision.	It is simple and fast.	Robustness depends on bounds on estimation errors.
Proposed Algorithm	Based on Symmetric Key Cryptography and LSB technique of Audio Steganography. No encoding on header of the Audio File.	Free from the damage of the header. Generates noiseless Stego File with 100% recovery.	If the length of the message increases beyond 5 digits, then difficult to handle. However, it is quiet impractical

5. COMPARISON ANALYSIS AMONG VARIOUS SYMMETRIC KEY CRYPTO-GRAPHY ALGORITHMS AND AUDIO STEGANOGRAPHY ALGORITHMS

The proposed algorithm basically tries to utilize the importance both the Network Security techniques namely Cryptography and Steganography. In this section, the efficiency of the proposed algorithm has been compared among various proposed existing algorithms, as drawn in Table.1.

In this section we have reviewed various papers on Symmetric key Cryptography, Audio Steganography as well as a combination of these algorithms. Every algorithm has certain advantages and disadvantages. Some algorithm uses XOR Logic while other uses LSB. Even many algorithms are there those can be applied to files beyond the Audio Files. But in many cases the recovery is not 100%. The complexities of many algorithms depend on the size of the message to be encrypted.

Some proposed Steganography algorithms also depends on the Audio File. Since neither Cryptography nor Steganography can individually secure the complete system, the proposed presents a combination of two. Combination of the two techniques provides a double layer security to the hidden message. While transmission, it neither creates any suspicion in hacker's mind nor does the latter could be able to retrieve the message easily.

6. CONCLUSION

Cryptography is the art of hiding a message by applying various encryption algorithms but the encrypted message creates suspicion on hacker's mind. Steganography is the process of concealing a message in another digital format. It may be an image, audio or video. A person on seeing the digital data cannot recognize the actual information behind it. This paper presents an algorithm on Audio Steganography with a combination of Symmetric Key Cryptography. The motive is to embed a message and send it through an insecure medium without any scope of extracting the underlying information. The algorithm does not encode the header part of the Audio File which ensures that even if the header got damaged it does not have any effect on the hidden information. Moreover, through experimental verifications, it has been proved that the Stego File generated is almost lossless which ensures 100% recovery of the original message. The algorithm provides robustness with a high degree of confidentiality and integrity.

7. FUTURE SCOPE

In this algorithm, only 5 bytes are used for storing the LSBs of the length of the original message and hence becomes difficult to handle if length exceeds more than 99999. Although it is quiet impractical for a secret message to be of size more than 99999 yet we shall try to solve such problem in our future works. We shall also try to implement this algorithm in various

file formats other than .mp3 to improve the efficiency of the algorithms.

REFERENCES

[1] Sourabh Chandra, Smita. Paira, Sk Safikul. Alam and Goutam Sanyal, "A Comparative Survey of Symmetric and Asymmetric Key Cryptography", *Proceedings of International Conference on Electronics, Communication and Computational Engineering*, pp. 83-93, 2014.

[2] Nedeljko Cvejic and Tapio Seppben, "Increasing the Capacity of LSB based Audio Steganography", *Proceedings of IEEE Workshop on Multimedia Signal Processing*, pp. 336-338, 2002.

[3] Anuradha, S. Kriti and Harish Kumar, "Audio Steganography Step toward the Secure Data Transmission: An Overview", *National Conference on Emerging Computing Technology*, 2010.

[4] Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems, Available at: www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf.

[5] Smita Paira, Sourabh Chandra, Sk. Safikul Alam and Siddhartha Bhattacharyya, "Symmetric Key Encryption Through Data Structure and Binary-Gray Conversion", *Emerging Research in Computing, Information, Communication and Applications*, Vol. 1, pp. 1-10, 2015.

[6] Symmetric-Key Cryptography, Available at: www.webopedia.com/TERM/S/symmetric_key_cryptography.html.

[7] Smita Paira, Sourabh Chandra, Sk. Safikul Alam and Siddhartha Bhattacharyya, "A Rotation Based Encryption Technique using Symmetric Key Method", *Emerging Research in Computing, Information, Communication and Applications*, Vol. 1, pp. 21-28, 2015.

[8] Pooja P. Balgurgi, and Sonal K. Jagtap, "Intelligent Processing: An Approach of Audio Steganography", *Proceedings of International Conference on Communication, Information and Computing Technology*, pp. 1-6, 2012.

[9] Jithu Vimal, and Ann Mary Alex, "Audio Steganography using Dual Randomness LSB Method", *Proceedings of International Conference on Control, Instrumentation, Communication and Computational Technologies*, pp. 941-944, 2014.

[10] Soumya Banerjee, Saikat Roy, M.S.Chakraborty and Simpita Das, "A Variable Higher Bit Approach to Audio Steganography", *Proceedings of International Conference on Recent Trends in Information Technology*, pp. 46-49, 2013.

[11] Vipul Sharmal, and Ravinder Thakur, "LSB Modification based Audio Steganography using Trusted Third Party Key Indexing Method", *Proceedings of* 3rd *International Conference on Image Information Processing*, pp. 403-406, 2015.

[12] Anu Binny and Maddulety Koilakuntla, "Hiding Secret Information using LSB based Audio Steganography", *Proceedings of International Conference on Soft Computing and Machine Intelligence*, pp. 56-59, 2014.

[13] Harish Kumar, and Anuradha, "Enhanced LSB Technique for Audio Steganography", *Proceedings of* 3rd *International Conference on Computing Communication and Networking Technologies*, pp. 1-4, 2012.

[14] Sourabh Chandra, Siddhartha Bhattacharyya, Smita Paira and Sk. Safikul Alam, "A Study and Analysis on Symmetric Cryptography", *Proceedings of International Conference on Science Engineering and Management Research*, pp. 1-8, 2014.

[15] P Jayaram, H.R Ranganatha and H.S. Anupama, "Information Hiding using Audio Steganography-A Survey", *The International Journal of Multimedia and its Applications*, Vol. 3, No. 3, pp. 86-96, 2011.

[16] Sorina Dumitrescu, Xiaolin Wu and Zhe Wang, "Detection of LSB Steganography via Sample Pair Analysis", *IEEE Transactions on Signal Processing*, Vol. 51, No. 7, pp. 1-27, 2003.

[17] Neha Gupta and Nidhi Sharma, "DWT and LSB based Audio Steganography", *Proceedings of International Conference on Reliability, Optimization and Information Technology*, pp. 428-431, 2014

[18] K. Thangadurai and G. Sudha Devi, "An Analysis of LSB based Image Steganography Techniques", *Proceedings of International Conference on Computer Communication and Informatics*, pp. 1-4, 2014.

[19] MPEG Audio Layer I/II/III Frame Header, Available at: www.mp3-tech.org/programmer/frame_header.html.