ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Steganography Algorithm to Hide Any Secret Message inside an Audio File

Asoke Nath[1], Sankar Das[2], Samriddhi Joshi[3], Saulat Daanyaal Alam[4], Alvin Roetgen[5]

Associate Professor, Dept. of Comp Sc, St. Xavier's College (Autonomous), Kolkata, India[1]

Assistant Professor, Dept. of Comp Sc, St. Xavier's College (Autonomous), Kolkata, India[2]

Final Year B.Sc. student, Dept. of Comp Sc, St. Xavier's College (Autonomous), Kolkata, India[3]

Final Year B.Sc. student, Dept. of Comp Sc, St. Xavier's College (Autonomous), Kolkata, India[4]

Final Year B.Sc. student, Dept. of Comp Sc, St. Xavier's College (Autonomous), Kolkata, India[5]

ABSTRACT: Steganography is a very important research area for hiding data inside some cover file. Many algorithms already developed for hiding secret message inside some image file. In the present work the authors propose a new method for hiding any encrypted secret message inside a cover file which may be any audio file. Before hiding secret message inside an audio file the secret message was encrypted using bit exchange algorithm. For hiding secret message inside different type of cover files Nath et al have already proposed various methods. In the present study the authors proposed to change LSB and LSB+3 bits and changing alternate bytes of the cover file. It means to hide one byte of secret message the authors used 8 bytes of the cover file but out of 8 bytes 4 bytes were modified in LSB and LSB+3 bit positions and the alternate bytes remain unchanged. The number of times the secret message to be encrypted using bit exchange method can be controlled by the user. The proposed bit exchange method is reversible that means the way the encryption done the decryption to be done in reverse way. The authors applied the present steganography algorithm on audio files and the result found was satisfactory. To embed any secret message inside a cover file the user has to enter a password and the same password to be used to unhide the secret message. The present method may be used for sending some secret key to someone over mail as the intruder may not be able to unhide and to decrypt the secret message.

KEYWORDS: Energy efficient algorithm; Manets; total transmission energy; maximum number of hops; network lifetime

I. INTRODUCTION

Steganography is the art of hiding information within safe cover carriers in ways such that the hidden message is undetectable. In Greek "stego" means "covered" or "secret" and "graphy" means "to write" and therefore "Steganography" becomes "secret or covered writing". The information to be hidden is embedded into the cover object which can be a text matter, some image or some audio/video file in such a way that the very existence of the message is undetected by maintaining the appearance of the resultant object exactly same as the original. The main goal of steganography is to hide the fact that the message is present in the Transmission medium.Data Hiding in audio signals is especially challenging, because the Human Auditory System (HAS) operates over a wide dynamic range. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than thousand to one. Sensitivity to additive random noise is also acute. The perturbations in a sound file can be detected as low as one part in ten million which is 80dB below ambient level. However, there are some 'holes' available. While HAS has a large Dynamic range, it has a fairly small differential range. As a result, loud sounds tend to mask out the quieter sounds. Additionally, the HAS is unable to perceive absolute phase, only relative phase. Finally, there are some environmental distortions so common to be ignored by the listeners.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

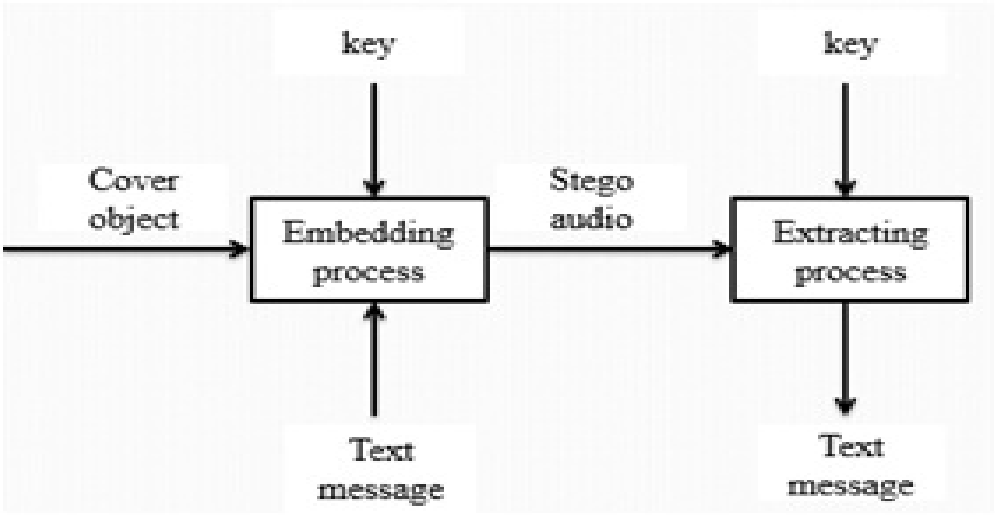

Figure 1-Steganography Process

Our objective is to come up with a technique of hiding the message in the audio file in such a way, that there would be no perceivable changes in the audio file after the message insertion. At the same time, if the message that is to be hidden were encrypted, the level of security would be raised to quite a satisfactory level.The proposed system uses Audio file as a carrier medium which adds another step in security. The objective of the newly proposed system is to create a system that makes it very difficult for an opponent to detect the existence of a secret message by encoding it in the carrier medium as a function of some secret key and that remains as the advantage of this system.Nowadays, several methods are used for communicating secret messages for defense purposes or in order to ensure the privacy of communication between two parties. So we go for hiding information in ways that prevent its detection. Some of the methods used for privacy communication are the use of invisible links, covert channels are some of existing systems that are used to convey the messages.Steganography is applicable to, but not limited to, the following areas.

1) Confidential communication and secret data storing
2) Protection of data alteration
3) Access control system for digital content distribution
4) Media Database systems

II. PROPOSED ALGORITHM

A. Methods used for embedding secret message file in the cover file:

Step-1: Encrypt the secret message file using simple bit shifting and XOR operation in the secret message file.
Step-2: Embed the encrypted secret message in the cover audio file in alternate byte positions. The bits in LSB and LSB+3 bits in the cover file were modified by the bits encrypted secret message.

B. Bit Exchange Encryption method:

Step-1: Read one byte from the secret message file and convert each byte to 8-bits. Apply 1 bit right shift operation on the entire file so that each byte will be modified accordingly.
Step-2: Divide 8-bits into two blocks 4 bits each and then perform the XOR operations with 4-bits on the left side with 4 bits on the right side and substitute the new bits in left 4-bit positions. The same thing repeated for all bytes in the file.
Step-3: Repeat step-1 by performing 2 bits right shift for all bytes in the secret message file. Then repeat step-2 again.

C. Steganography Algorithm:

In the present work authors have used the substitution of LSB and LSB+3 bits of the cover file in alternate bytes. The last 300 bytes of the cover file is used to store password and size of the secret message file. To embed encrypted secret

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

message file one byte of encrypted secret message file is taken and convert it into 8 bits and then 2 bits of the encrypted secret message were taken and then substitute in the LSB and LSB+3 bits of the cover file and then leave one byte of the cover file unchanged. The same process repeated for all 8 bits of the secret message. In the present algorithm the last 300 bytes of the cover file are not tampered at all. The size of the secret message file must be less than 10% of the cover file.

To make the system secured one has to enter some password while embedding an encrypted secret message. If password is correct then the program will read the file size from the cover file and start to work on the cover file. To extract the secret message one has to perform exactly the reverse process of the encryption method. The program first matches the password. If it is correct then it will read the size of the secret message file from the embedded cover file. Then it will read 8 bytes and extract 8 bits from 4 alternate bytes and convert them to a character and write onto an external file. Once all bytes extracted from the cover file then decryption program to be executed get back the original secret message file.

III. RESULTS AND DISCUSSION

Sl. No.	Cover file type	Secret file type used
1.	.WAV	Text File
2.	.MP3	Text File

Table 1: Results and Discussions

The present method was applied on different cover files and secret message files and the results obtained are given below:

(i) **Case-1:** WAV file

Cover_File(musical108.wav: Size=128KB)) + Secret_mesage(Text File: Size=3.12KB) → Embedded File(output108.wav: Size= 128KB)

(ii) **Case-2:** Mp3 file

Cover File + Fig_3: Secret message = Fig_4:Embedded Cover File Name=1.mp3
File name = a.txt Name=2.mp3
(Size=5.32MB) (Size=4KB) (Size=5.32MB)
(The encrypted secret message file is embedded)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

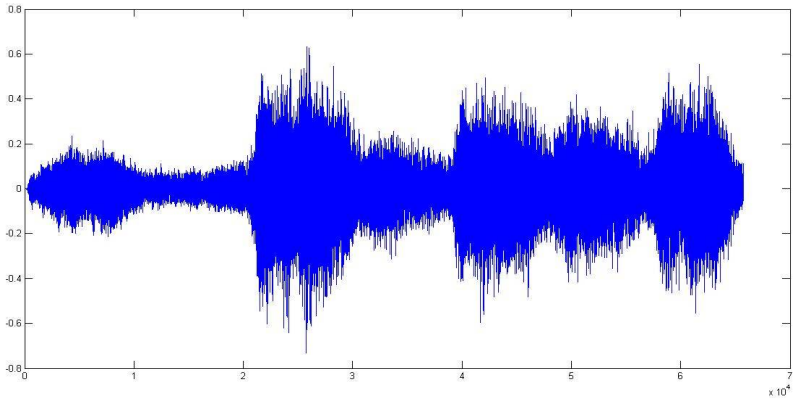

Figure 2: The Cover file before embedding

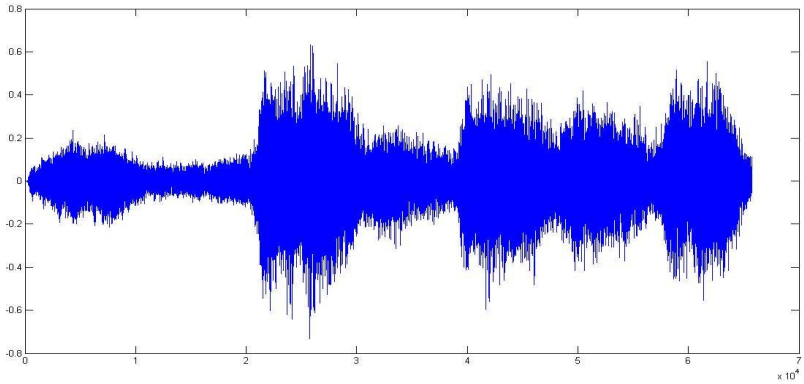

Figure 3: The Cover file after embedding

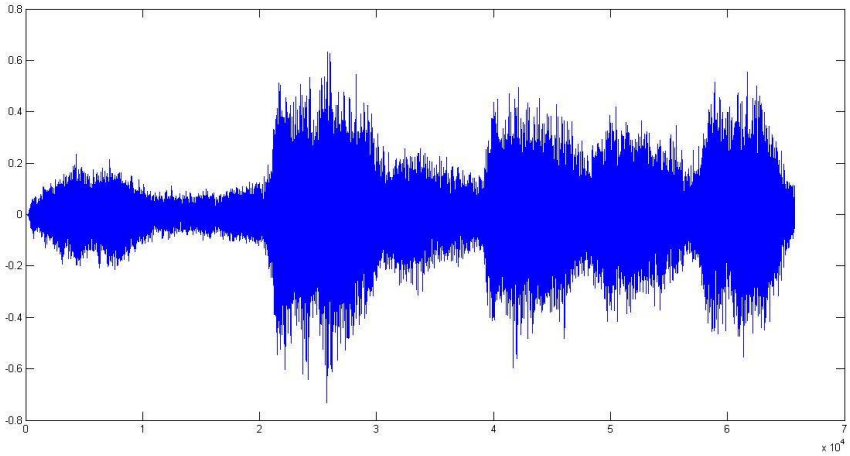

Figure 4: The Cover file after extraction is completed

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

IV. CONCLUSION AND FUTURE SCOPE

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Audio file Steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at Steganography to circumvent such policies and pass messages covertly.Although the algorithm presented is a simple one and not without its drawbacks, it represents a significant improvement over simplistic stenographic algorithms that do not use keys. By using this algorithm, two parties can be communicated with a fairly high level of confidence about the communication not being detected.In designing the "Steganography" utmost care was taken to meet user requirements as much as possible. The analysis and design phase was reviewed. Care was taken strictly to follow the software engineering concepts and principles so as to maintain good quality in the developed system as per the user requirements.Hiding information may introduce enough visible noise to raise suspicion. Therefore the carrier or cover audio must be carefully selected. A cover audio should contain some randomness. It should contain some natural uncertainty or noise. Once it has been used, the audio should be used again and should be destroyed. A familiar audio should be used. It is better for the steganographer to create own audios. This proposed system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. Encryption and Decryption techniques have been used to make the security system robust. The project is being well made to tackle the security issues and user interface makes user to handle well the system and provides good communication between user and the system. The encrypt key makes further security and available of different audio formats to choose by the user makes project a valuable project. As the encoding method varies dynamically, it can't be determined and hence even when the existence of message is detected, it can't be read. To a steganalysis expert unable to determine the chosen encoding, a bit is just a bit. A better function can be determined to improve the ability of the technique. Combining still more steganography methods may improve the strength of the technique. Future Work: We are going to implement this application for compressed audio file formats and large audio files by using same technique.In the present work some secret message has been embedded inside a cover file in encrypted form so that no one will be able to extract actual secret message. The programs have been developed in MATLAB. LSB and LSB+3 bits of the cover file have been embedded in every alternate byte position. The encryption of the secret message file here has been taken 5 times but one can go up to any limit .If the encryption number is increased then the process becomes slow but the encryption will be very strong. In principle it will be difficult for any one to decrypt the encrypted message without knowing the exact encryption method. This method is essentially stream cipher method and it may take huge amount of time if the files size is large and the encryption number is also large. This present method may be most suitable for water marking. The Steganography method may be further secured if the secret message is first compressed ,then encrypted and then finally embedded inside the cover file.

REFERENCES

1. www.garykessler.net/library/steganography.html
2. http://www.frontlinedefenders.org/manual/en/esecman/chapter2_8.html
3. http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00.html
4. www.aes.org/events/113/papers/I.cfm
5. en.wikipedia.org/wiki/WAV
6. www.borg.com/~jglatt/tech/wave.htm
7. https://audiostegano.wordpress.com/category/requirement-analysis/
8. Agniswar Dutta, Abhirup Kumar Sen, SankarDas , Shalabh Agarwal and AsokeNath :New Data Hiding Algorithm in MATLAB using Encrypted secretmessage : Proceedings of IEEE CSNT-2011 held at SMVDU (Jammu), 03-06 Jun, 2011

BIOGRAPHY

Dr. Asoke Nath is Associate Professor in the Department of Computer Science, St. Xavier's College(Autonomous), Kolkata. Dr. Nath involved in research work in Cryptography and Network Security, Steganography, Green Computing, Mathematical modelling of social networks, Big data analytics, Cognitive Radio, Data Science, e-learning, MOOCs etc. He has published more than 185 papers in Journals and conference proceedings.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Prof. Sankar Das is Assistant Professor in the Department of Computer Science, St. Xavier's College(Autonomous), Kolkata. Prof. Das is involved in research area such as Steganography, Visual Cryptography, Image processing etc. Prof. Das published several papers in Journals and proceedings of conferences.

Samriddhi Joshi is a final year BSc Computer Science Honours student from St. Xavier's College, Kolkata. Apart from her studies ,she is interested in the field of 3D animation and Steganography.

Saulat Daanyaal Alam is a final year BSc Computer Science student from St.Xavier's college,Kolkata. Apart from his studies he is interested in the field of steganography.

Alvin Roetgen is a final year BSc Computer Science student from St.Xavier's college ,Kolkata. Apart from his studies he is interested in the field of steganography.