EFFICIENT DATA HIDING SCHEME USING AUDIO STEGANOGRAPHY

Mohit Kulkarni[1], Maitreyee Phatak[2], Uma Rathod[3] , Sudhir Prajapati[4,],

[1234] BE IT, Department of Information Technology, RMD Sinhgad School of Engineering, Pune, Maharashtra, India.

Mrs.Shivganga Mujgond [5]

[5]Assistant Professor, Department of Information Technology, RMD Sinhgad School of Engineering, Pune, Maharashtra, India.

---***---

Abstract - ***Steganography is essentially a security system which is utilized to shroud the private or mystery information. This mystery information is inserted or hid in a manner that no other individual separated from the sender or beneficiary can seize it. Audio Steganography is a piece of steganography in which the spread media utilized is a sound document, by changing a data in an intangible way. The cryptographic strategies in audio steganography "scramble" messages so if caught, the messages can't be comprehended, while, inserting, "covers" a message to shroud its presence and concealing the way that a message is being sent out and out. Inserting is not expected to supplant cryptography but rather supplement it and it is a more perplexing system. Presently, because of the accessibility of repetition the first message before inserting and the stego message after extraction continues as before, in this manner keeping up its trustworthiness. Audio Steganography can accomplish security, protection, privacy and information respectability. The information which is covered up can be a content document, sound or a picture. The current Slightest Critical Piece (LSB) procedure is one of the most straightforward methodologies for secure information exchange. This calculation has a noteworthy escape clause that it is anything but difficult to split the messages that are covered up in the spread media. The proposed calculation, that is, Computerized Encryption Framework, is more secure and empowers proficient private correspondence in the middle of sender and recipient. The proposed calculation joins encryption and embedding.***

Keywords : Steganography, Audio Steganography, Stego File, Cover Audio, Embedding.

1. INTRODUCTION

The word Steganography originates from the Greek word "Steganos" which implies secured composing. Steganography is the procedure of concealing data such that its vicinity can't be distinguished. Steganography conceals the information as well as shrouds the way that correspondence is occurring. The mystery data is encoded in such a way, to the point that the very presence of the data is disguised. Along these lines it can be said that, steganography can be utilized to complete concealed trades.

Steganography uses interactive media content as host and installs mystery data that is imperceptible to any onlooker other than the planned beneficiary. Along these lines arranged sight and sound records can be uninhibitedly appropriated over the web without raising suspicion, and is utilized by malignant gatherings to facilitate exercises, release mystery or very touchy data, and that's only the tip of the iceberg.

The principle motivation behind Steganography calculations is to stow away however much data inside of the spread media as could reasonably be expected. Consequently, for steganography calculations the tradeoff is between the measure of secretive data being inserted, regularly called as Stego information, and the affirmation that its vicinity and substance be undetected.

The primary objective of Steganography is to convey safely in a totally imperceptible way and to abstain from attracting suspicion to the transmission of a shrouded information. It is not to keep others from knowing the concealed data, however it is to keep others from suspecting that the data even exists. Steganographic calculation are known as most mystery and strong methods for installing shrouded data into the spread media without changing the nature of the host signal.

2. RELATED WORK DONE

In the audio steganography, system won't change the span of the record even in the wake of encoding furthermore suitable for a sound document design. Calculations utilized as a part of LSB insertion method are effortlessly decryptable.

A brief depiction of how mix of cryptography and steganography to secure information while transmitting in system is given. On the off chance that the examination between various calculations such as AES, DES and RSA is done, AES calculation is observed to be more secure than others and less tedious. Some of the time the sound records might get tainted.

Information using so as to stow away should be possible advanced images. One approach to secure the responsibility for computerized picture is to furtively install information in the substance of the picture recognizing the proprietor. Throughout the years, there have been numerous improvements in information stowing away, particularly as it relates to assurance of computerized pictures. The spread or host is the medium in which the message is implanted and serves to shroud the vicinity of the message. This is likewise alluded to as the message wrapper. The stego picture ought to take after the spread picture under easygoing examination and investigation. For recouping the message, it likewise requires a deciphering key. Procedures that endeavor to insert data just in a perceptually immaterial way, for example, LSB installing strategies, are helpless against having the implanted information misshaped or quantized by lossy picture pressure.

The reason for steganography is hosting an undercover correspondence between two gatherings whose presence is obscure to a conceivable assailant, a fruitful assault comprises in recognizing the presence of this correspondence. Copy-right checking, rather than steganography, has the extra necessity of strength against conceivable assaults. Security should be possible through lack of clarity, cover, concealing the area of installed data, spreading the shrouded data and so forth. In this way, both verifiable point of reference and late development give us an extensive variety of instruments, which if connected keenly ought to be adequate to take care of the greater part of the security issues that one needs to confront in current circumstances.

A data theoretic model for steganography with latent foes is proposed. The contrast between detached enemies and dynamic foes is clarified. A model of stego framework is given wherein, sender changes spread content to contain an inserted message E utilizing a mystery key K. The yield of the concealing procedure is the stego-content S. The collector must have the capacity to recuperate from his insight into the stego-content S and from the key K. The passsive aggressor does not know whether sender sends true blue spread content C or stego-content S containing shrouded message.

The data theoretic model and other measurable methodologies will at last be more helpful for determining proclamations about the security of data covering up.

3. PROPOSED METHOD

With help of Audio Steganography method, we are going to create one desktop application it will give high security to the private information and it will likewise be useful for discharge correspondence between two users such as sender and beneficiary with the assistance of emit key. Audio Steganography is a system used to transmit concealed data by adjusting a sound sign in a subtle manner. Firstly, audio file will be encoded with help of key, 128bits. In the wake of scrambling the sound record, pressure will apply and sound document will pack under 24MB. Subsequent to handling, message inserting is done and after that it will be sent over the system to the planned collector. Beneficiary will take after the converse method to get unique message. In this system of audio steganography, some measure of commotion arrives when the information is implanted, the recurrence of clamor is changed by a few bits yet that change is extremely insignificant and it is quiet. Thusly, the sound record which is sent to the recipient will be of a decent quality and the collector will get the information productively.

3.1 SYSTEM ARCHITECTURE

Fig shows the actual detailed representation of system architecture of Audio Steganography is given and how our project works right from the start till the end, with all the minute details. . Above all else, the sender chooses the data record which can be as sound, content or picture. The extent of the data message will be not exactly the span of spread sound record. This spread record must be in .mp3 document format. Sender will encode the information with the assistance of key, where key size is 128bit. In the spread sound document, sender will implant the compacted message and send the sound record. This key is same for sender and collector. On the collector's side, the recipient will get the sound record through the system, then concentrate the information from the sound document with help of key, decompress it lastly unscramble the message to get it in its unique structure. At the sender's side, the first information experiences the stages like pressure, encryption and implanting in order to be secure and safe from the meddler or regardless of the possibility that the busybody seizes information, he can't change over it in the first frame. Along these lines, the mixed, installed information is of no utilization to the busybody, in this manner satisfying the rationale of the undertaking.

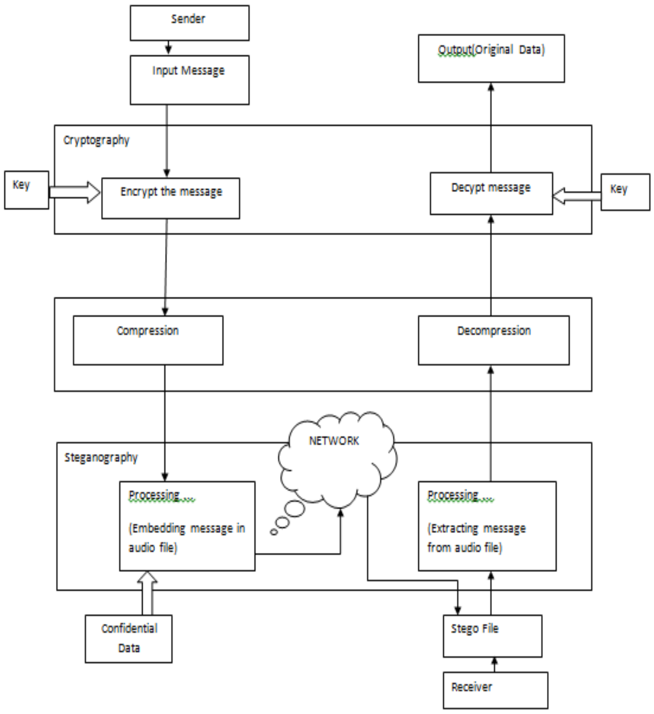


Fig 1 : System Architecture

3.2 COMPONENTS OF PROPOSED SYSTEM

I. ENCRYPTION MODULE

The encryption module is capable of encoding the original data in the communication. It is used to scramble text in a form which the normal person cannot read. Also, encryption is done with help of key where the key size for our algorithm is of 128bits.

II. EMBEDDING

In embedding, the confidential data is embedded or hidden in an audio file in such a way that it cannot be visible to the third person. Embedding is the most important step in audio steganography. When the data is embedding, the frequency of noise is changed by some bits but that is very negligible change and it is not audible to a human ear.

III. STEGO FILE

Stego file is the processed file which the sender sends through a network. The original data file, after being embedded becomes a stego file. This stego file is extracted from the audio file by the receiver to view the original message.

IV. COMPRESSION

Compression is done to reduce the size of the given file less than 24MB. It is commonly used in many applications for memory management. It is done by sender.

V. DECOMPRESSION

Decompression is exactly opposite to compression. The decompression is done to view original data in its original size.

VI. EXTRACTION MODULE

It is done at receiver side. The receiver extracts the embedded data from audio (cover) file with help of key.

VII. DECRYPTION MODULE

Decryption is the decoding of the scrambled data to its original form.

4. EXPERIMENTS AND RESULTS

After performing various experiments, the following observations are taken :

The carrier file should be strictly audio (.mp3) file format and the secret message may be of image or text file.

Here for our experimental scenario the carrier audio file is COVER.*mp3* of 24 MB size .

For secret file (image or text),

1. for text – file format should be .txt

2 .for image- the input file should be .JPEG (provided it is lossy)

3.for audio-cover file should be .mp3

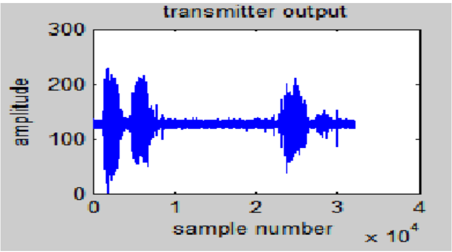
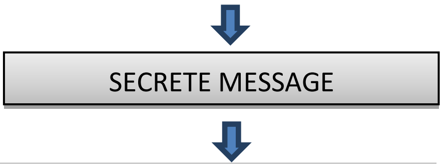


Fig 2: Carrier Audio File


SECRETE MESSAGE

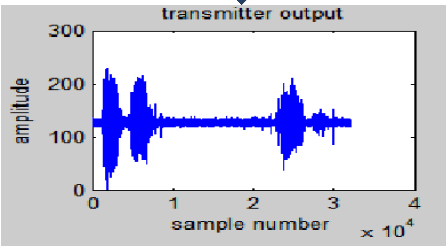


Fig 3: Stego Audio File to be Transmitted

The COVER file is *COVER.mp3* of 4.20MB size. The secret image file is *Joker.JPEG* of 31.8KB size. The secret text file is *Hello.txt* of 20 KB size. Thus the carrier file must be greater than the secret message file.

Various embedding techniques make noise while the data is being hidden.

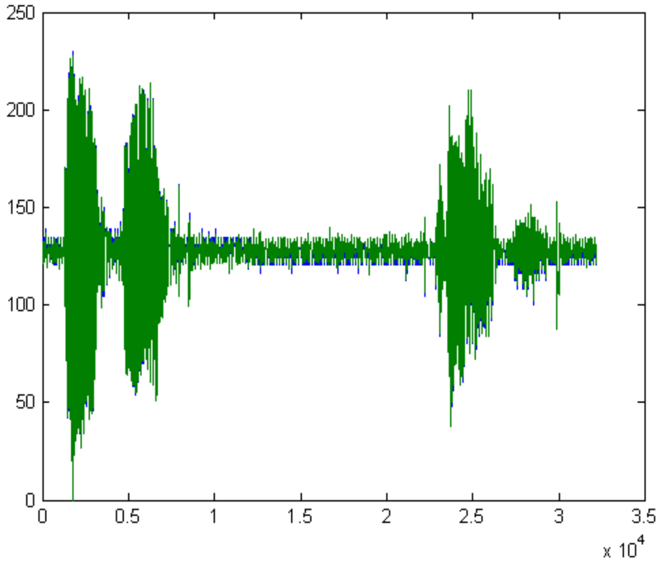


Fig 4: Comparison of Original cover Audio File and Stego Audio File

COMPARISON : Above figure shows the comparison between original file before the secret data is embedded in it ,and the file after the secret data is embedded in it.

	Cover File	Secret Data File Format	Stego File
File Name	COVER.mp3	Hello.txt Joker.JPEG	COVER.mp3
Size	4.20MB	20KB 31.8KB	4.2OMB 4.20MB

Table No.1 : While Embedding Data.

	Stego File	Retrieved secret data	Cover File
Name	COVER.mp3	Hello.txt Joker.JPEG	COVER.mp3
Size	4.20MB	24KB 190KB	4.20MB

Table No.2 : After Retrieving Data

5. CONCLUSION

Steganography particularly joined with cryptography, is a capable apparatus which empowers individuals to impart without conceivable meddlers not withstanding knowing there is a type of correspondence in any case. These strategies utilized as a part of the art of steganography have propelled a great deal over the previous hundreds of years, particularly with the ascent of PC period. The proposed strategy is a device which permits the client to install the content or picture or a sound record information in a spread media which is only a sound sign under a solitary stage.

6. ACKNOWLEDGEMENT

We take this chance to thank our task guide Ms. Shivganga Mujgond and Head of the Department Ms. Sweta Kale for their significant direction and for giving all the fundamental offices, which were basic in the finishing of this venture report.

We are likewise grateful to all the staff individuals from the Department of Information Technology of RMD Sinhgad School of Engineering, Warje for their profitable time, bolster, remarks, recommendations and influence. We might likewise want to thank the establishment for giving the required offices, Internet access and imperative books.

7. REFERENCES

[1] Michel Kulhandjian, Dimitris Pados, "Extracting Spread-Spectrum Hidden Data from Digital media", IEEE transactions on information forensics and security VOL:8 NO:7,July 2013.

[2] B hagyashri Patil, Vrishali Chakkarwar, "Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach" IOSR Journal(ISOR-JCE),VOL:9 Issue 1, Jan–Feb 2013.

[3] B.Padmavathi, S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique", International

Journal of Science and Research, Volume 2 Issue 4, April 2013.

[4] Fahimeh Rezaei,Tao Ma et.l, “An anti-steganographic approach for removing secret information in digital audio data hidden by SS methods” IEEE transaction on system security symposium,978-1-4673-3122-7/13/$31.00 ©2013 IEEE, 2013.

[5] E.T. Lin and E.J. Delp, "A Review of Data Hiding in Digital Images," in Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, PICS '99, Ed.pp. 274—278, April 1999.

[6] F.A.P Peticolas, R.J. Anderson and M.G. Kuhn, “Information Hiding – A Survey”, in proceeding of IEEE, pp. 1062-1078, July 1999.

[7] C. Cachin, “An Information-Theoretic Model for Steganography”, in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, May 1998.