International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 03 – Issue 04 || April 2018 || PP. 46-51

Audio Steganography

P. H. Govardhan, Aniket Giradkar, Ankit Dekate, Digvijay Raut, Dnyaneshwar Nagrikar
Computer Science and Engineering
Priyadarhini Institute of Engineering and Technology
Rashtrasanth Tukadoji Maharaj Nagpur University

Abstract: The paper special treatment on Audio Steganography using JAVA is the application developed to embed a Text data in to another audio signal. It is worried with embedding information in an offensive cover Speech in a secure and robust manner and malicious attack. This system makes the Files more secure by using the concepts Steganography. In this Steganography the secret messages are fix in wave sound. The not known message is fix by slightly change in character the binary particular of a sound file. Attaching secret messages in wave sound is usually a more tough process than attaching messages in other media. In order to hide secret messages successfully, a variety of steps taken in order to achieve for attaching information in wave audio have been introduced. These techniques range from rather simple process that attach information in the form of signal noise to more powerful methods that exploit having signal processing techniques to hide information.

Keywords: Audio Steganography, JAVA, Data Hiding

1. Introduction

The main purpose for preparing this document is to give a general insight into the analysis and requirements of the existing system or situation and for determining the operating characteristics of the system. The main objective of the system main focus will be on Secret communication. The main part is that the advisory is does not and should not know that there is a secret message embedded in the content. This Document plays a vital role in the development life cycle (SDLC). As it describes the complete requirement of the system. It is meant for use by the developers and will be the basic during testing phase. Any changes made to the requirements in the future will have to go through formal change approval process. A method of embedding information in the Cestrum domain of a cover audio signal is described for audio steganography applications. The proposed technique combines the commonly employed psycho acoustical masking property of the human auditory system with the decorrelation property of the speech cestrum, and achieves imperceptible embedding, large payload, and accurate data retrieval. Results of embedding using a clean and a noisy hot utterance show the embedded information is robust to additive noise and bandpass filtering. Now that a full description of the first embodiment has been described via a detailed example, it is appropriate to point out the rationale of some of the process steps and their benefits.

he ultimate benefits of the foregoing process are that obtaining an identification number is fully independent of the manners and methods of preparing the difference image. That is to say, the manners of preparing the difference image, such as cutting, registering, scaling, etcetera, cannot increase the odds of finding an identification number when none exists; it only helps the signal-to-noise ratio of the identification process when a true identification number is present. Methods of preparing images for identification can be different from each other even, providing the possibility for multiple independent methodologies for making a match.

2. Objective

The main objective of the project Audio steganographyis to embed the text message in cover audio file, using the available methods of audio steganography methods. The receiver extracts the message from carrier audio file.

3. System Anaylsis

The system analysis can be defined in terms of Data Flow Diagram.
There are two types of DFD's they are

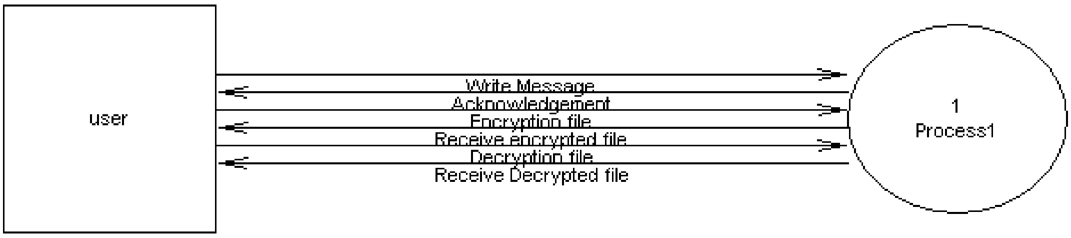
1) Context Level DFD
2) Top Level DFD

Context Level DFD:

In the Context Level the whole system is shown as a single process.

- No data stores are shown.

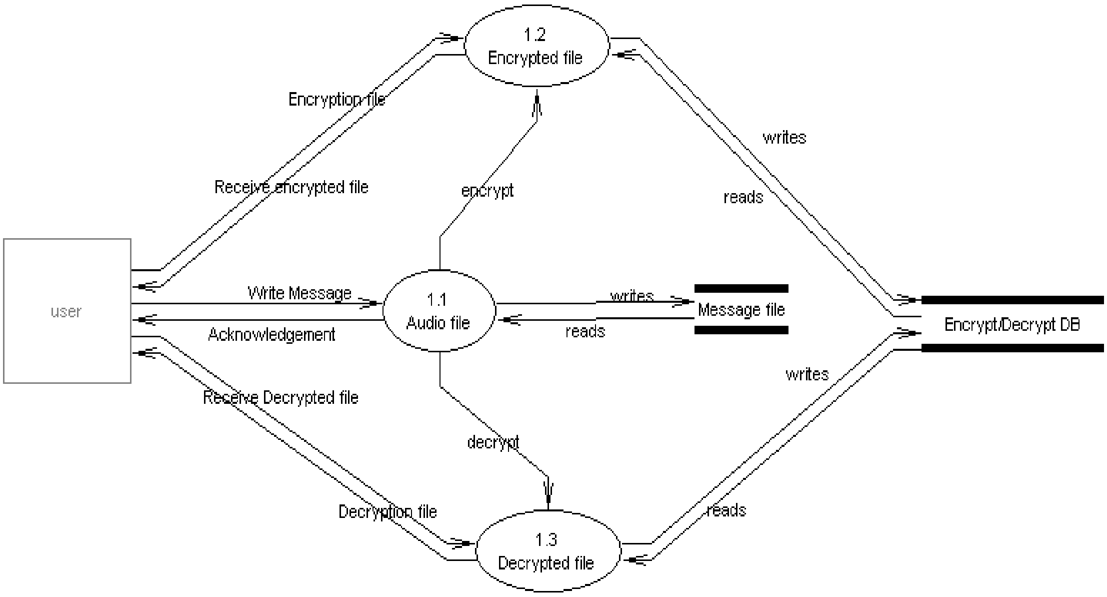
- Inputs to the overall system are shown together with data sources (as External entities).
- Outputs from the overall system are shown together with their destinations (as External entities).



3.1 Context Level DFD

Top Level DFD:

The Top Level DFD gives the overview of the whole system identifying the major system processes and data flow. This level focuses on the single process that is drawn in the context diagram by 'Zooming in' on its contents and illustrates what it does in more detail.



3.2 Top Level DFD

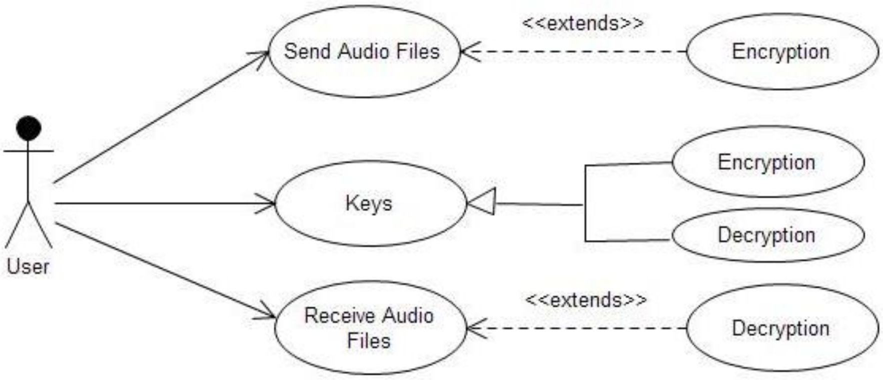
4. Implemenatation

This can be done with the help of Admin Module i.e. easy to manage your survey in the field.
The Functionalities of the Administrator is:

1. The administrator should login into the system with unique his/her password and username.
2. If the username and password is validated then he can gain access to the system.
3. Admin applies the Steganography concepts to the users file.
4. writes message and Encrypts the with the key
5. Decrypts the message

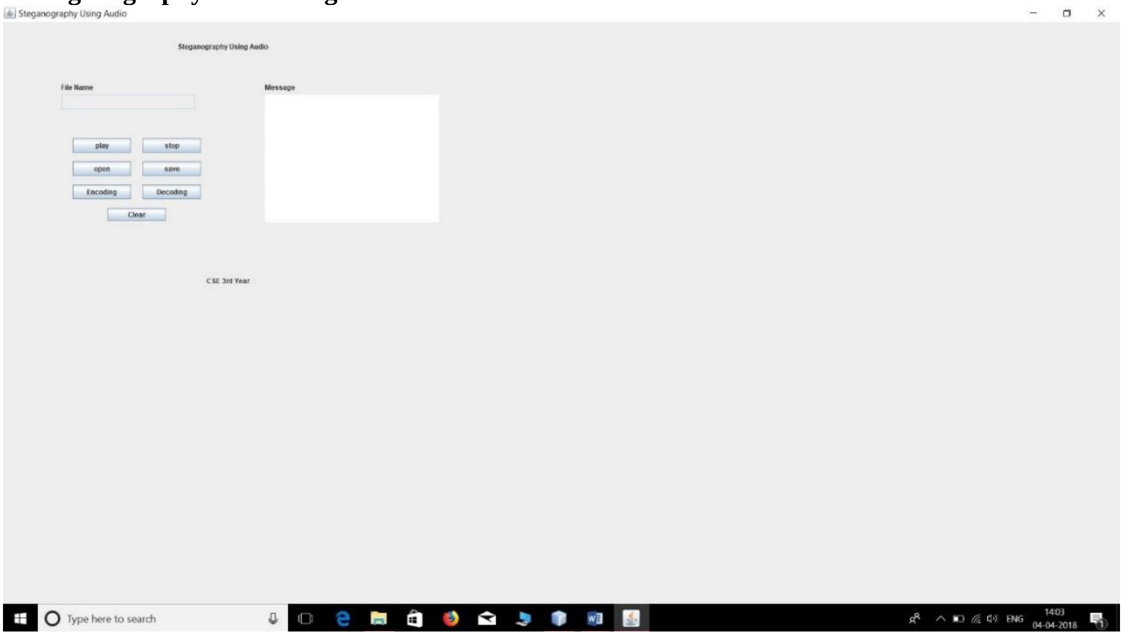
The Administrator can do the following actions:

1. Register
2. Login
3. Change Password
4. Admin Actions
   - Receives the message
   - Applies the Steganography concepts
   - Forwards the message to the concerned user.
   - Sends the message(File)
   - Receive the message(File)

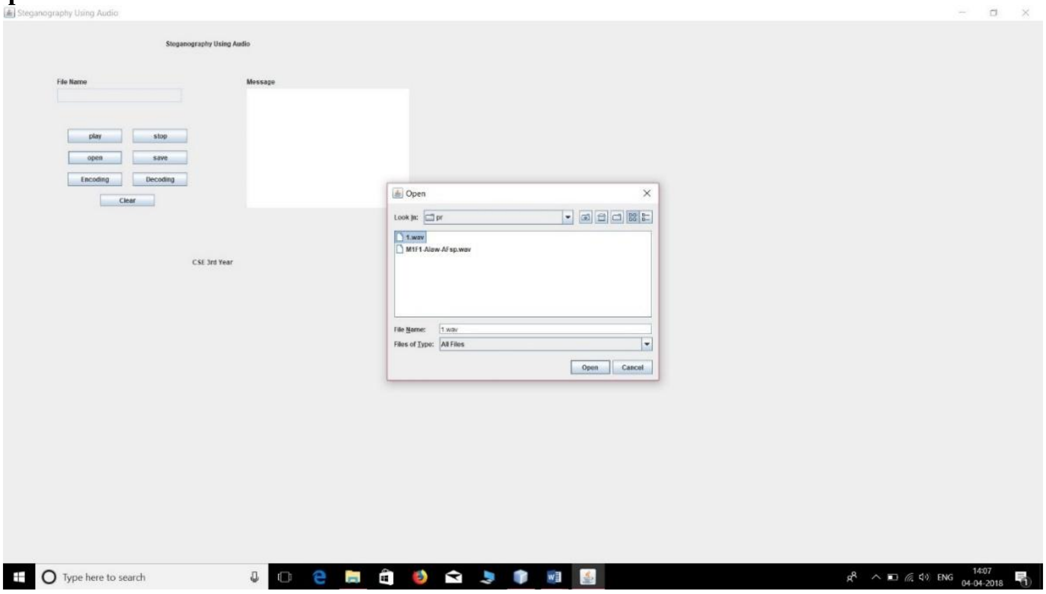


4.1 Working Diagram

Audio Steganography: Home Page



Click Open Button and select .wav file

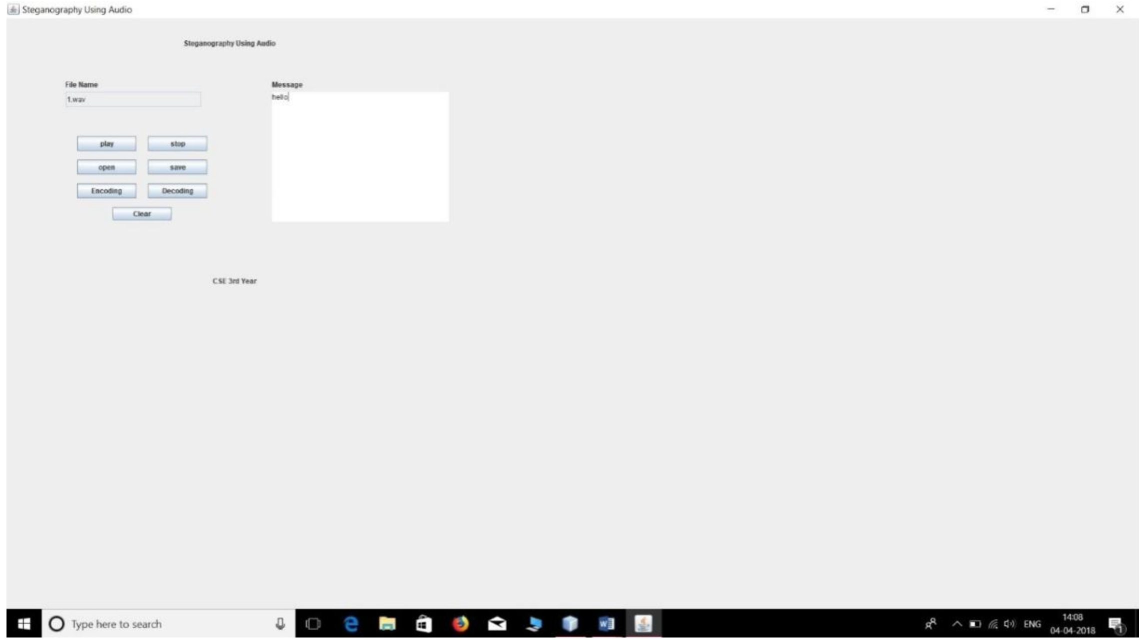


Look In: pr

1.wav
M1F1-Alaw-AFsp.wav

File Name: 1.wav
Files of Type: All Files

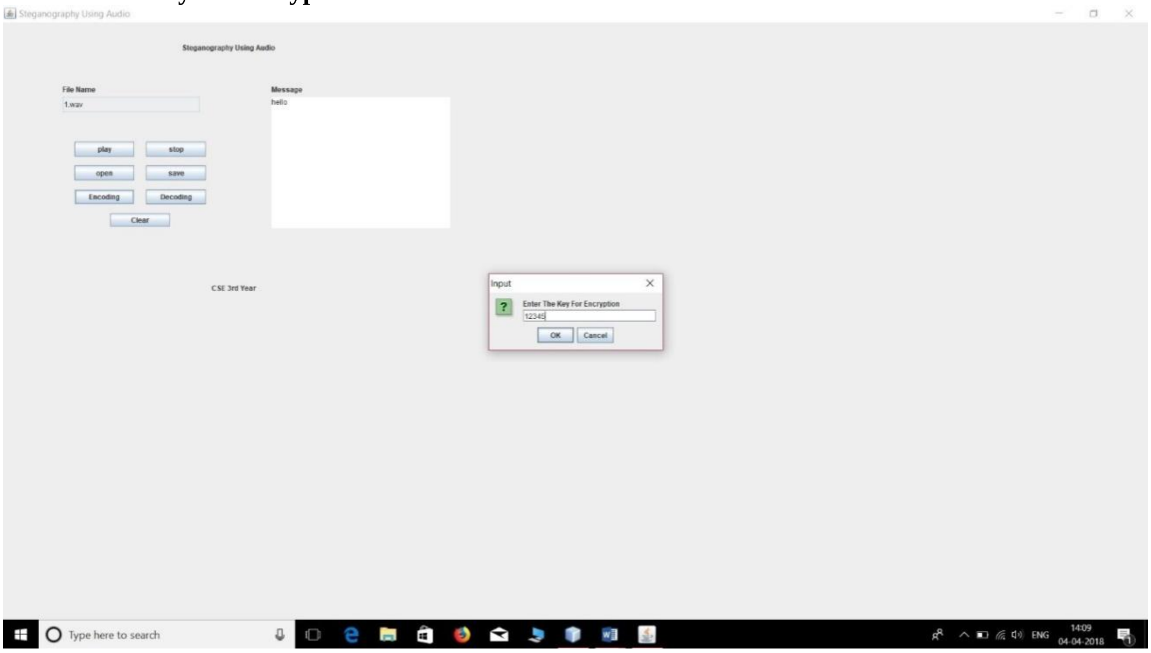
Write Your Text Here



File Name
1.wav

Message
hello

Then Enter the key for encryption and click Ok and close.

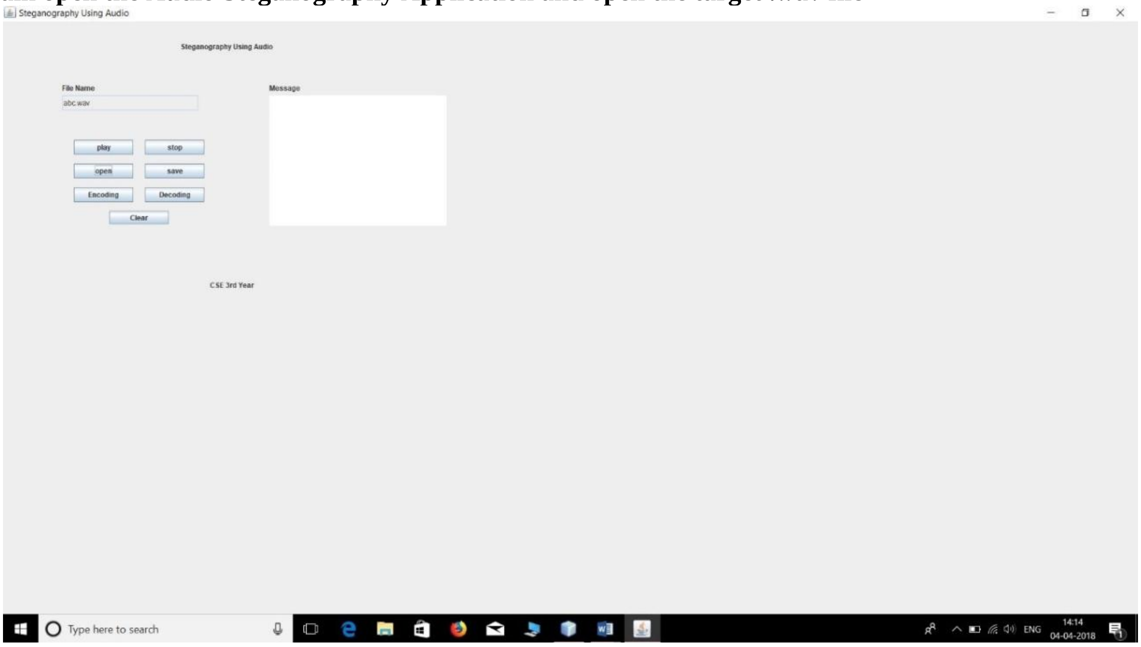


File Name
1.wav

Message
hello

Enter The Key For Encryption
12345

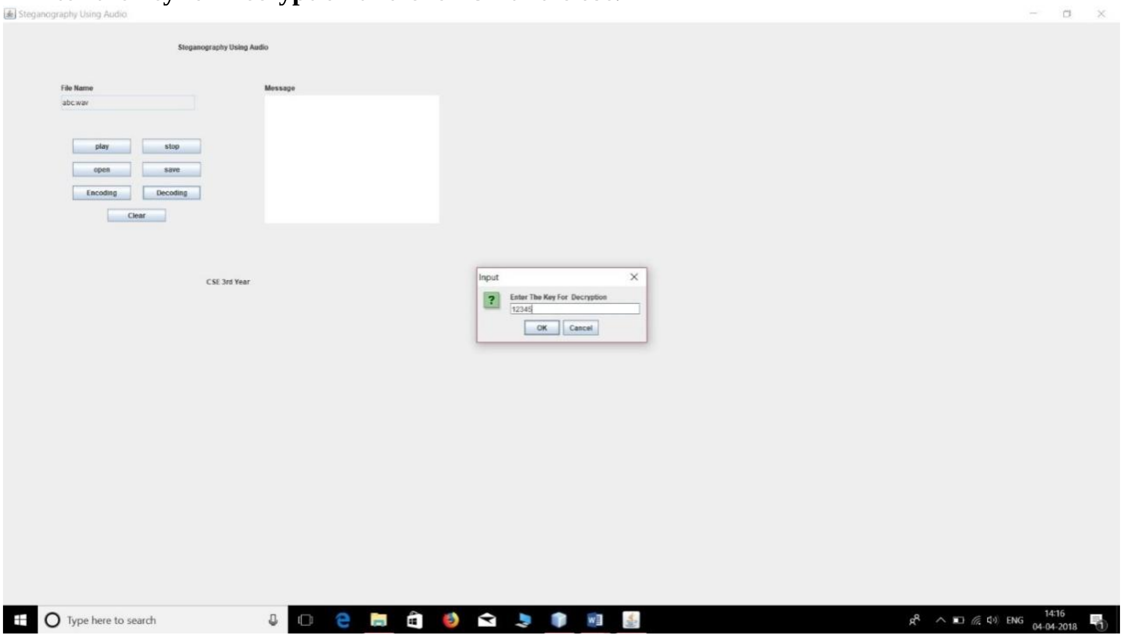
Again open the Audio Steganography Application and open the target .wav file



Steganography Using Audio

File Name: abc.wav

Then Enter the key for Decryption and click Ok and close.



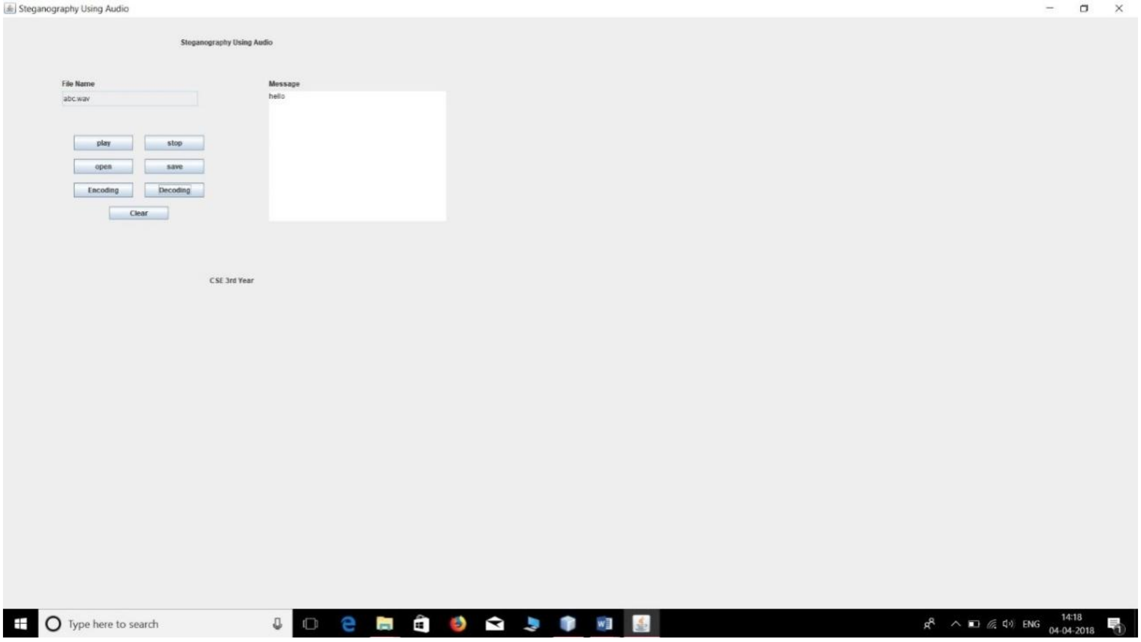
Steganography Using Audio

File Name: abc.wav

Input

Enter The Key For Decryption: 12345

Output will Displayed



File Name
abc.wav

Message
hello

5. Conclusion

In this study, an audio steganalysis technique is proposed and tested. These methods used in the science of steganography have advanced a lot over the past centuries, especially with the rise of computer era. Although the techniques are still not used very often, the possibilities are endless. Many different techniques exist and continue to be developed, while the ways of detecting hidden messages also advance quickly.