STEGANOGRAPHY USING AUDIO IN REMOTE MONITORING SYSTEM

A PROJECT

Submitted to

DEPARTMENT OF COMPUTER ENGINEERING

For the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER ENGINEERING

Under the Supervision of

Ms Divya Chaudhary

By

Sarthak Goel 349/CO/15

Sarthak Srivastava 350/CO/15

DEPARTMENT OF COMPUTER ENGINEERING

NETAJI SUBHAS INSTITUTE OF TECHNOLOGY
2017

NETAJI SUBHAS INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER ENGINEERING

Nov,2017

Certificate

This is to certify that this project report entitled STEGANOGRAPHY USING AUDIO IN REMOTE MONITORING SYSTEM by Sarthak Goel (349/CO/15) and Sarthak Srivastava (350/CO/15), submitted in partial fulfillment of the requirements for the degree of Bachelor of Engineering in Computer Engineering under Netaji Subhas Institute of Technology, during the academic year 2017, is a bonafide record of work carried out under my guidance and supervision.

Ms Divya Chaudhary
Assistant Professor
Department of Computer Science and Engineering

Table of Contents

1. Introduction

1.1 Definition

Steganography is used to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hiding copyright notice or serial number or even help to prevent unauthorized copying directly.The sender embedsdata of any type in a digital cover file using a key to produce a stego-file, in such a way that an observer cannot detect the existence of the hidden message. At the other end, the receiver processes the receivedstego-file to extract the hidden message. An obvious application of such stenographic system is a covertcommunication using innocuous cover audio signal, such as telephone or videoconference conversations. To minimize the difference between the cover and the stego-medium, recent steganography techniquesutilize natural limitations in human auditory and visual perceptions.

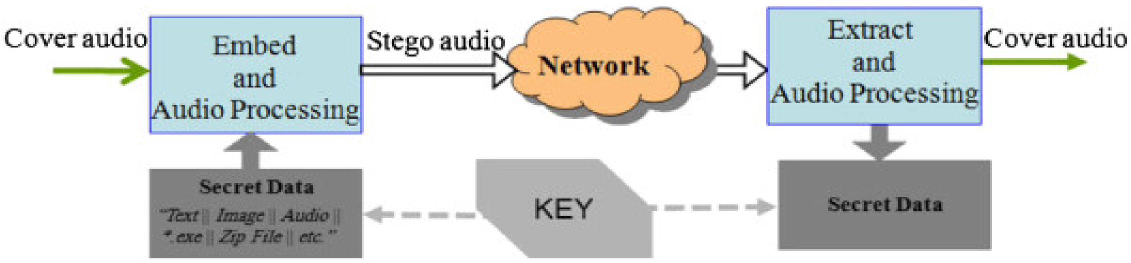

Cover audio
Embed and Audio Processing
Stego audio
Network
Extract and Audio Processing
Cover audio
Secret Data
"Text || Image || Audio || *.exe || Zip File || etc."
KEY
Secret Data

Figure-1 Audio Steganography flow

1.2 Motivation

The internet allows for easy dissemination of information over large areas. This is both a blessing and a curse since friends all over the world can view your information but so can everyone else. Encrypting data has been the most popular approach to protecting information but this protection can be broken with enough computational power. An alternate approach to encrypting data would be to hide it by making this information look like something else. This way only friends would realize its true content. In particular, if the important data is hidden inside of an image then everyone but your friends would view it as a picture. At the same time your friends could still retrieve the true information. This technique is often called data hiding or stenography.

1.3 Overview

There is the server part, which waits for clients connections and for each connected client, a new frame appears showing the current client screen. When you move the mouse over the frame, this results in moving the mouse. When you click any Particular client screen then it is automatically zoom out. You can easily watch it is activity. After that when you click on cancelled button then it is automatically go to previous screen short.

Remote Server is the server part, which waits for clients connections and for each connected client, a new frame appears showing the current client screen. When you move the mouse over the frame, this results in moving the mouse. When you click any Particular client screen then it is automatically zoom out. You can easily watch it is activity. After that when you click on cancelled button then it is automatically go to previous screen short.

Remote Clients core function is sending a screen shot of the client's desktop every predefined amount of time. It also receives server commands such as "move the mouse command", and then executes the command at the client's PC.

It has one more feature; we can send any message from server to any client.

- The message transfer System is meant to keep the security of the message send between servers to clients in a LAN.
- You can send any message from server to any clients.
- The main concern of this project is to improve the efficiency and effectiveness of the whole system.

The existing system of Audio Steganography poses more restrictions on the choosing of audio files. User can select only wav files to encode. Further embedding information into sound files isgenerally considered more difficult than images; according to the human ear is extremely sensitive to perturbations in sound and can in fact detect such turbulence as low as one part in 10 million. The four methods discussed further provide users with a large amount of choice and makes the technology more accessible to everyone.

2. Literature Review

2.1 Remote Monitoring

The Remote Network Monitoring (RMON) MIB was developed by the IETF to support monitoring and protocol analysis of LANs. The original version (sometimes referred to as RMON1) focused on OSI Layer 1 and Layer 2 information in Ethernet and Token Ring networks. It has been extended by RMON2, which adds support for Network- and Application-layer monitoring which adds support for switched networks. It is an industry standard specification that provides much of the functionality offered by proprietary network analyzers. RMON agents are built into many high-end switches and routers. [2]

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. An RMON implementation typically operates in a client/server model. Monitoring devices (commonly called "probes" in this context) contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients. While both agent configuration and data collection use SNMP, RMON is designed to operate differently than other SNMP-based systems:

- Probes have more responsibility for data collection and processing, which reduces SNMP traffic and the processing load of the clients.
- Information is only transmitted to the management application when required, instead of continuous polling. [8]

In short, RMON(REMOTE MONITORING) is designed for "flow-based" monitoring, while SNMP is often used for "device-based" management. RMON is similar to other flow-based monitoring technologies such as NetFlow and Sflow because the data collected deals mainly with traffic patterns rather than the status of individual devices. One disadvantage of this system is that remote devices shoulder more of the management burden, and require more resources to do so. A minimal

RMON agent implementation could support only statistics, history, alarm, and event.[9]

2.2 Steganography using Audio

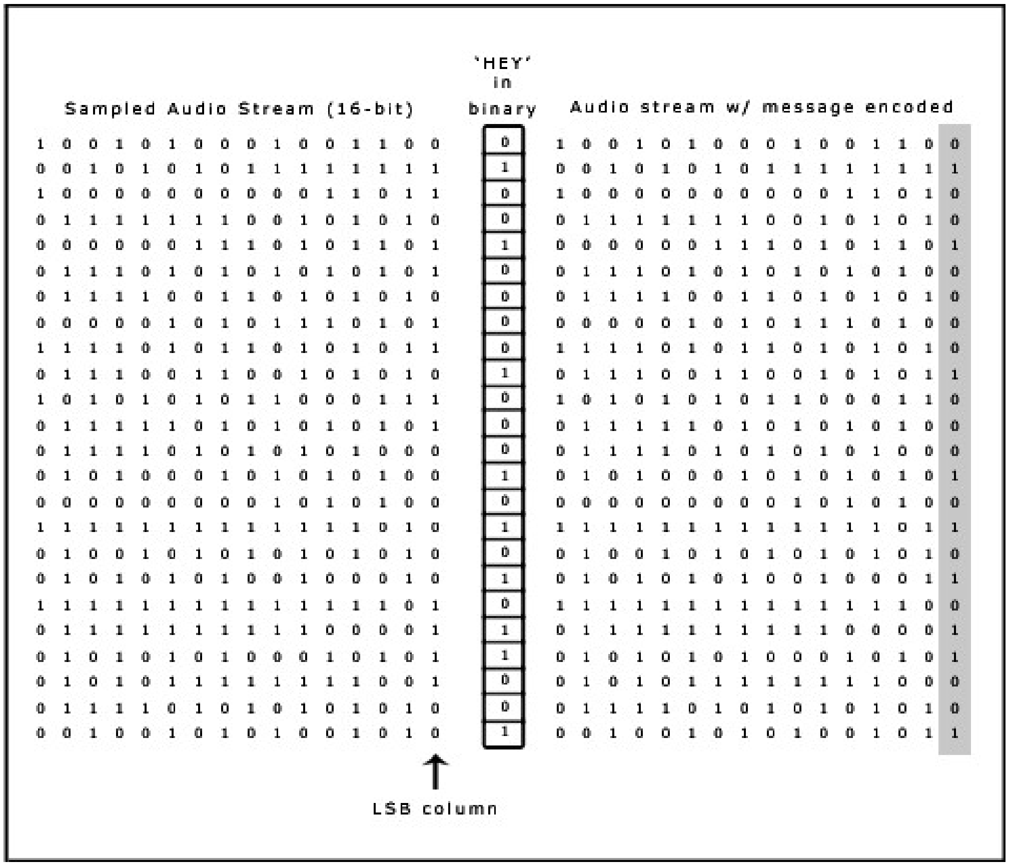
In a computer-based audio Steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio Steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information.

Thus the main purpose of this report is to explain Audio Steganography and algorithm commonly employed for Audio Steganography and its applications.[12]

2.3 Algorithm

2.3.1 LSB Coding

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method:



```
                                                  'HEY'
                                                    in
   Sampled Audio Stream (16-bit)                 binary    Audio stream w/ message encoded
1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0                   0        1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0
0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1                   1        0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1
1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 1                   0        1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0
0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0                   0        0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0
0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1                   1        0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1
0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1                   0        0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0                   0        0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0
0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 1                   0        0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 0
1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 1                   0        1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 0
0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 0                   1        0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 1
1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 1                   0        1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 0
0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 1                   0        0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0                   0        0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0
0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 0                   1        0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1
0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0                   0        0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0
1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0                   1        1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1
0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0                   0        0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 0                   1        0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1                   0        1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0
0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1                   1        0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1
0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1                   1        0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1
0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 1                   0        0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0                   0        0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0
0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 0                   1        0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 1
                              ↑
                         LSB column
```

Figure 2 - (LSB Algorithm)

It performs bit level manipulation to encode the message. The following steps are

a. Receives the audio file in the form of bytes and converted in to bit pattern.

b. Each character in the message is converted in bit pattern.

c. Replaces the LSB bit from audio with LSB bit from character in the message.[14]

2.3.2 LSB-2 Coding

If the message bit to be embedded is 0, then adjust the LSB such that the XOR operation on LSB and next to LSB is 0 and if the message bit to be embedded is 1, then adjust the LSB such that the XOR operation on LSB and next to LSB is 1 [15]

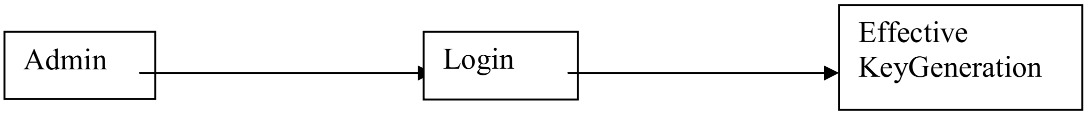
3. Proposed Approach

3.1 Flow Chart

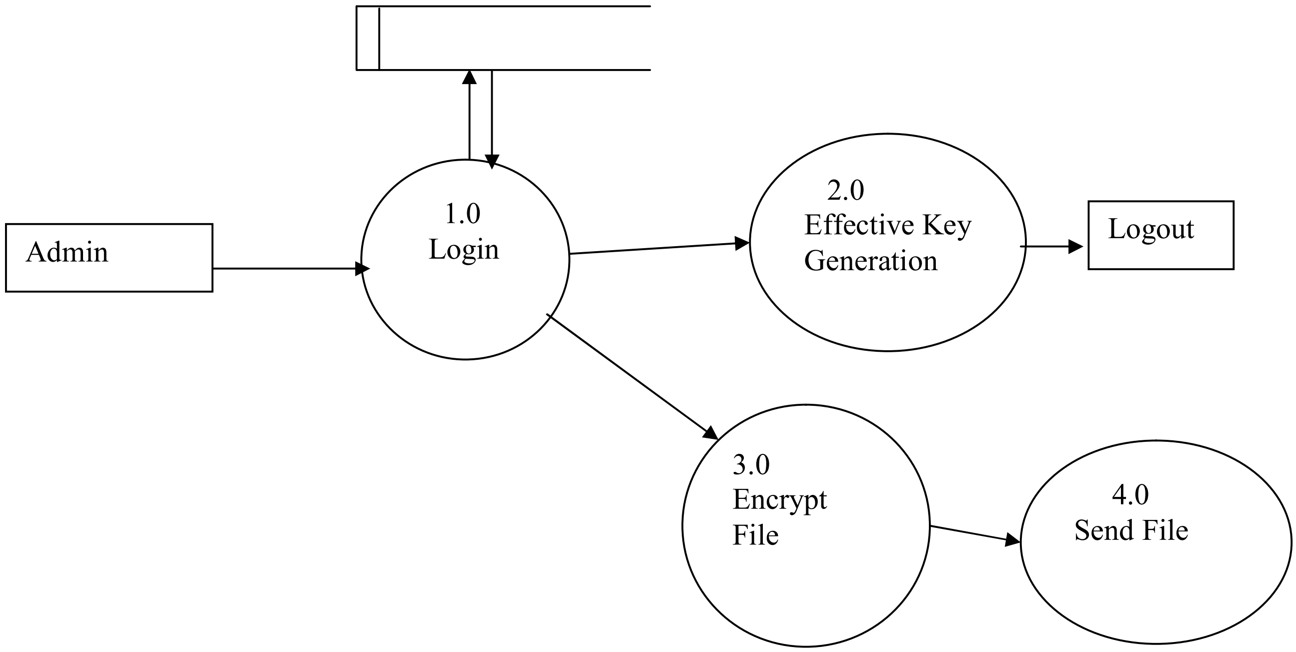
The following flow charts represent the flow of control in the system.

Element References	Symbols
Data Flow Process	→
Process	○
Data Store	⊏
Source or Sink	□

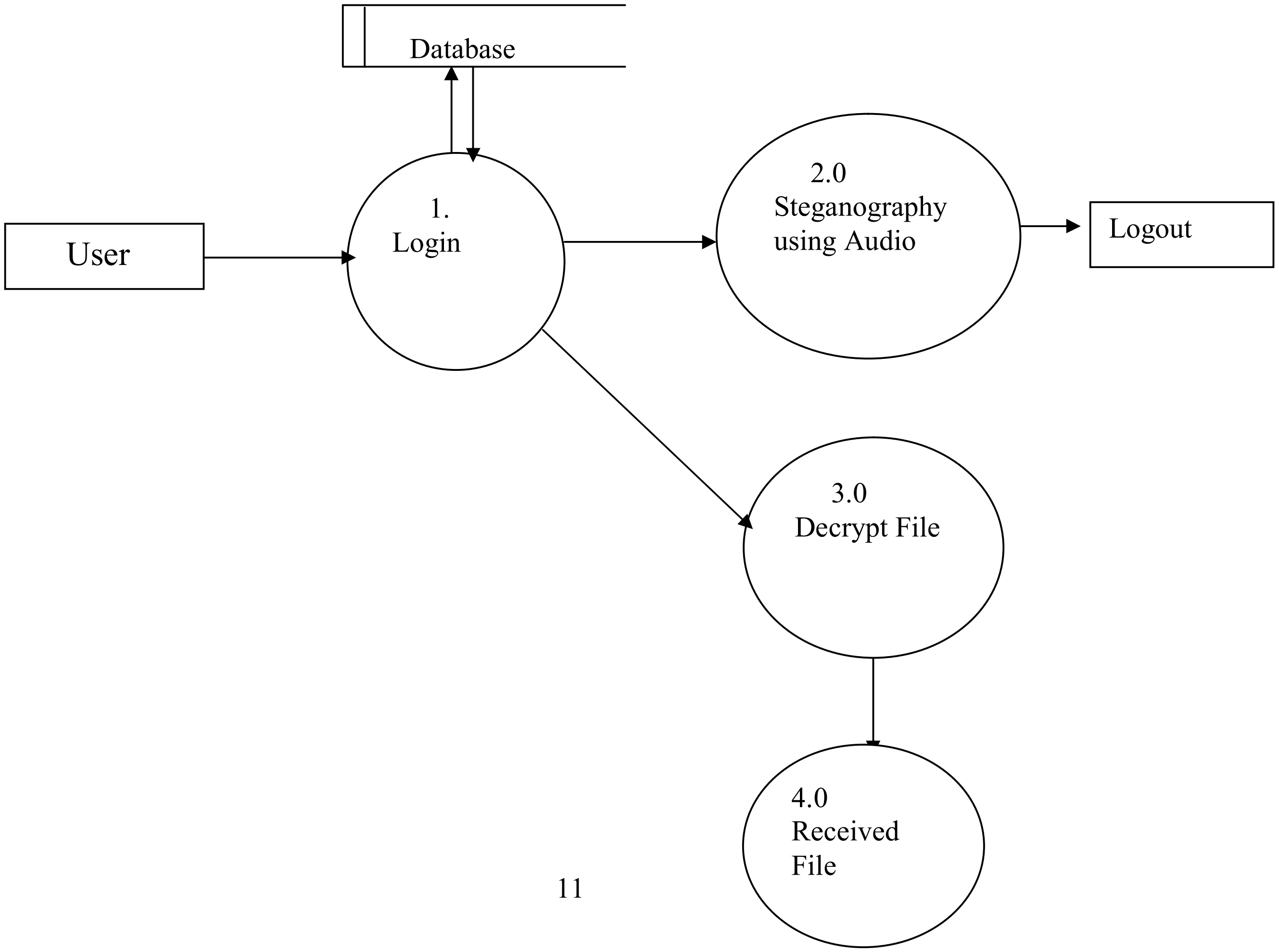
3.1.1 Zero Level



3.1.2 First level (Admin)



3.1.3 First level (User)



4. Results and Analysis

4.1 Experimental Setup

4.1.1 Hardware Specification

Processor	:	Intel P-III based system
Processor Speed	:	250 MHz to 833MHz
RAM	:	64MB to 256MB
Hard Disk	:	2GB to 30GB
Software Specification:		
Language	:	JDK 1.5, Net beans 7.3/6.9 ,Java
Operating System	:	Any Operating System.

4.1.2 Software Specification

Operating System	:	Windows 7/xp/windows8/10
Languages	:	java 2(EJB2.0, JDBC, JSP, Servlet, Java Mail)
Front End	:	Core java
Platform	:	J2EE
Web Servers	:	Web Logic8.1/Apache Tomcat 8.0
Backend	:	My SQL
Browser Program	:	Google Chrome/Mozilla Fireworks

4.2 Comparisons

Table 1: Comparison between Steganography and Cryptography

STEGANOGRAPHY	CRYPTOGRAPHY
Unknown message passing	Known message passing
Prevents discovery of the very existence of communication.	Prevents an unauthorized party from discovering the contents of communication.
Technology still being developed for various formats.	Most of the algorithms are known by all.
Once detected message is known, it does not alter the structure of the secret message.	It alters the structur of the secret message
Less known Technology	Commonly known Technology.

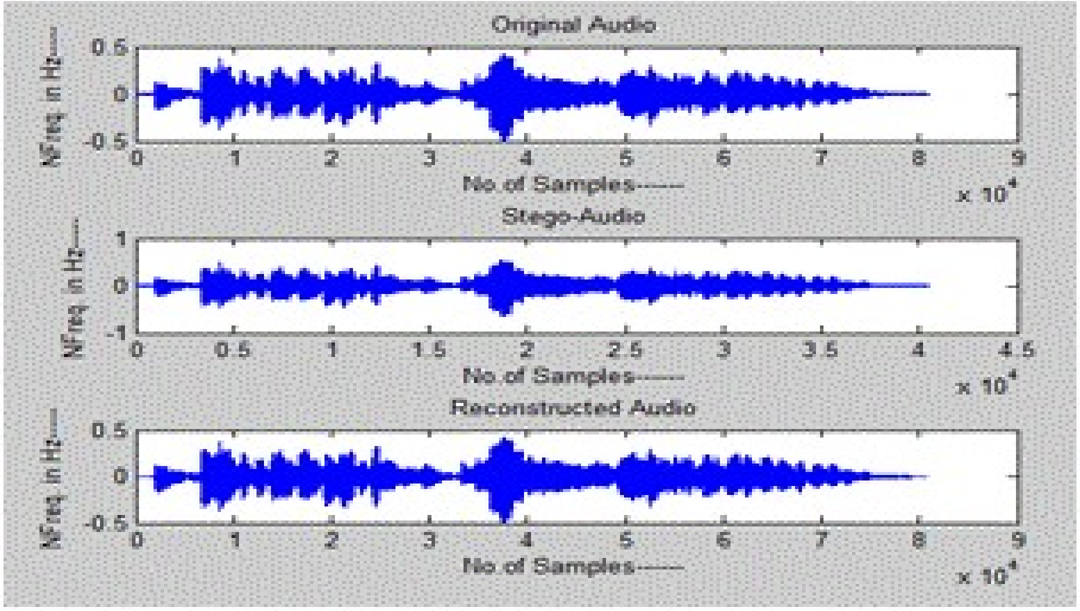


Fig 3: Output of proposed audio steganography scheme

4.3 Analysis

Availability

System availability means the amount of time that the system can work continuously and properly without any interruption. This specification can be made because in some systems downtime can be required to perform specific tasks such as upgrades and backups of the system. In this system, because it will be used by thousands of users, officers, and administrators, the downtime must be eliminated.

Efficiency

This aspect is important in developing the crime file management system because a large amount of data will be stored in it and retrieved from it.

Flexibility

System flexibility means how easy the system is in terms of maintenance; in this system, a number of functionalities are expected to increase after deployment, to extend the capability of the system and to perform additional tasks. In each system, this aspect should be planned from the beginning. Therefore, it can be considered in the design of this system.

Portability

System portability means a system has the capability of being deployed on any hosting service provider. In developing the crime file management system, the java scripting language is used so it can be run on the majority of web servers.

Security

Generally, the web-based system can be accessed by various users to find different information. Hence, on the home page of this system, a validation form is provided to separate users' capabilities according to their authenticity in the system. The main reason for doing this is to prevent unauthorized access to the system. For this reason, mySQL Server commands were used to protect the system from unauthorised users.

5. Conclusion

Steganography provides means for secure data transmission and secure data storage network. Therefore, important files carrying confidential information can be stored in the server in an encrypted form. Access to these files is limited to certain authorized people only. Transmission also takes place in an encrypted form so that no intruder can get any useful information from the original file during transit. Further, before trying to access important files, the user has to login to the system using a valid username and password, which is allotted to him by the system administrator.

Experimental results show that LSB 2-bit technique shows lesser values of MSE, RMSE, percentage of bytes changed and AFCPV for embedding audio message as secret message as compared to LSB coding audio message as secret message as the total number of bytes for text message are lesser than the total number of bytes of message image which means that more amount of text message can be embedded.

6. References

[1] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn:”Information Hiding- A Survey”, Process of IEEE, vol.87, no.7, pp.1062-1078, July, 1999.

[2] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, “Techniques for data hiding”, IBM Systems Journal, Volume 39 , Issue 3-4, July 2000, pp. 547 – 568.

[3] Neil F.Johnson, Z.Duric and S.Jajodia. “Information Hiding Steganography and Watermarking-Attacks and Countermeasures”,Kluwer Academic Publishers, 2001

[4] NedeljkoCvejic, TapioSeppben “Increasing the capacity of LSB-based audio steganography ” FIN- 90014 University of Oulu, Finland ,2002.

[5] Min Wu, Bede Liu. “Multimedia Data Hiding”, Springer- Verlag New York, 2003.

[6] Robert Krenn, “Steganography and steganalysis”, An Article, January 2004.

[7] R.A. Santosa and P. Bao, “Audio-to-image wavelet transform based audio steganography,” Proc. Of 47th Int. Symposium ELMAR, June 2005, pp. 209- 212.

[8] Xuping Huang, Ryota Kawashima, NorihisaSegawa, Yoshihiko Abe. “The Real-Time Steganography Based on Audio-to-Audio Data Bit Stream”,Technical report of IEICE, ISEC, vol.106 pp.15-22, September 2006.

[9] Aoki, Naofumi. ”A Band Widening Techniquefor VoIP Speech Using Steganography Technology”, Report of IEICE, SP,106(333), pp.31-36, 2006.

[10] N. Taraghi-Delgarm, “Speech Watermarking”, M.Sc. Thesis, Comptuer Engineering Department, Sharif University of Technology, Tehran, IRAN, May 2006.

[11] M. Pooyan, A. Delforouzi, “LSB-based Audio Steganography Method Based on Lifting Wavelet Transform”, in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.

[12] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya, Poulami Das, DebashisGanguly and Swarnendu Mukherjee, “A tutorial review on Steganography”, International Conference on Contemporary Computing (IC3-2008), Noida, India, August 7-9, 2008, pp. 105-114.

[13] SajadShirali-Shahreza M.T. Manzuri-Shalmani “High capacity error free wavelet domain speech steganography” ICASSP 2008

[14] Navneet Kaur Int. Journal of Engineering Research and Applications, ISSN : 2248-9622, Vol. 4, Issue 6(Version 5), June 2014, pp.94-100

[15] http://shodhganga.inflibnet.ac.in/bitstream/10603/9089/7/07_chapter%203.pdf, July,2016