**KANTIPUR ENGINEERING COLLEGE**

**(Affiliated to Tribhuvan University)**

**Dhapakhel, Lalitpur**



**[Subject Code: CT755]**

**A MINOR PROJECT FINAL REPORT ON**

**“AUDIO IN IMAGE STEGANOGRAPHY”**

**Submitted by:**

**Amar Raj Bahik [78407]**

**Bubaneshwor Prasad Yadav [78415]**

**Manil Maharjan [78436]**

**Sarba Raj Shrestha [78470]**

**A MAJOR PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF BACHELOR IN COMPUTER OR ELECTRONICS & COMMUNICATION ENGINEERING**

**Submitted to:**

**Department of Computer and Electronics Engineering**

**March, 2021**

**AUDIO IN IMAGE STEGANOGRAPHY**

**Submitted by:**

**Amar Raj Bahik [78407]**

**Bubaneshwor Prasad Yadav [78415]**

**Manil Maharjan [78436]**

**Sarba Raj Shrestha [78470]**

**Supervised by:**

**Supervisor Name**

**(Designation of supervisor)**

**A MAJOR PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF BACHELOR IN COMPUTER OR ELECTRONICS & COMMUNICATION ENGINEERING**

**Submitted to:**

**Department of Computer and Electronics Engineering**

**Kantipur Engineering College**

**Dhapakhel, Lalitpur**

**March, 2021**

**COPYRIGHT**

The author has agreed that the library, Kantipur Engineering Collage, may make this report freely available for inspection. Moreover the author has agreed that permission for extensive copying of this project report for scholarly purpose may be granted by the lecturers, who supervised the project works recorded herein or, in their absence, by the Head of Department wherein the project report was done. It is understood that the recognition will be given to the author of the report and to the Department of Computer and Electronics, KEC in any use of the material of this project report. Copying or publication or other use of this report for financial gain without approval of the Department and author’s written permission is prohibited. Request for permission to copy or to make any other use of the material in this report in whole or in part should be addressed to:

Head

Department of Computer and Electronics Engineering

Kantipur Engineering College

Dhapakhel, Lalitpur

Nepal

**KANTIPUR ENGINEERING COLLEGE**

**DEPARTMENT OF COMPUTER AND ELECTRONICS ENGINEERING**

**APPROVAL LETTER**

The undersigned certify that they have read and recommended to the Institute of Engineering for acceptance, a project report entitled “AUDIO IN IMAGE STEGANOGRAPHY” submitted by Amar Raj Bahik, Bhubaneshwar Prasad Yadav, Manil Maharjan and Sarba Raj Shrestha in partial fulfillment for the degree of Bachelor of Engineering in Computer Engineering.

…………………………..

Supervisor

Name of Supervisor

Designation of Supervisor

……………………….

External Examiner

Name of External Examiner

Designation of External Examiner

…….……………………...…

Er. Rabindra Khati

Head of Department

Department of Computer and Electronics Engineering

Date:  **ACKNOWLEDGEMENT**

It gives us immense pleasure to express our deepest sense of gratitude and sincere thanks to our highly respected and esteemed guide Er. Nischal Khadka for his valuable guidance, encouragement and help. His useful suggestions for this whole work and cooperative behavior are sincerely acknowledged. We would like to express our sincere thanks to Er. Bishal Thapa for his technical assistance. As a coordinator of the minor project for the 3rd year, his presence has been immensely commendable. We would also thank Er. Ankit Adhikari for his guidance throughout this project. We would also like to thank Er Rabindra Khati (Head of Department of Computer and Electronics and Communication) for his support. At the end we would like to express our sincere thanks to all our friends and others who helped us directly or indirectly during this project.

**-**

**ABSTRACT**

Nowadays, data has become the most valuable part of any individual or organizations.

Steganography is the art of hiding the fact that communication is taken place, by hiding information in other information. Stronger steganographic techniques are needed to ensure the integrity of data stored on a machine that may be infected or under attack. The objective of this project is to communicate secret audio message between sender and receiver. This program makes more difficult for anyone who tries to break the security to get hold of the hidden audio information. Steganography usually deals with the ways of hiding the existence of the communicated data in such a way that it remains confidential. It maintains secrecy between two communicating parties.

This project hides the secret audio information by generating RGB image of secret audio information. Here we are using .WAV audio file format. By using raw data of audio information, we generate an RGB image. The generated image will contain the audio information without losing its information. The generated image is sent to destination with the help of private or public communication network. On the other side, receiver download the generated image using the software and retrieve the secret audio information.

**Key Word:** Stronger steganographic techniques, under attack, secret audio message, security, confidential, .WAV audio, RGB image.

TABLE OF CONTENTS

[ABSTRACT i](#_Toc29452037)

[LIST OF FIGURES v](#_Toc29452038)

[CHAPTER 1: INTRODUCTION 1](#_Toc29452039)

[1.1 Background 1](#_Toc29452040)

[1.2 Problem Statement 2](#_Toc29452041)

[1.3 Objectives 3](#_Toc29452042)

[1.4 Applications 3](#_Toc29452043)

[1.5 Project Features 3](#_Toc29452044)

[1.6 Feasibility Analysis 3](#_Toc29452045)

[1.6.1 Economic Feasibility 4](#_Toc29452046)

[1.6.2 Technical Feasibility 4](#_Toc29452047)

[1.6.3 Operational Feasibility 4](#_Toc29452048)

[1.7 System Requirement 4](#_Toc29452049)

[1.7.1 Software Requirement 4](#_Toc29452050)

[1.7.2 Hardware Requirement 5](#_Toc29452051)

[1.7.3 Functional and Non-Functional Requirement 5](#_Toc29452051)

[CHAPTER 2: LITERATURE STUDY 6](#_Toc29452052)

[2.1 Steganography 6](#_Toc29452053)

[2.2 History of Stenography 6](#_Toc29452055)

[2.3 Current system analysis and proposed system 7](#_Toc29452055)

[2.3.1 Current System 7](#_Toc29452056)

[2.3.2 Proposed System 8](#_Toc29452057)

[CHAPTER 3: METHODOLOGY 9](#_Toc29452058)

[3.1 Embedding System 9](#_Toc29452059)

[3.2 Extraction System 12](#_Toc29452065)

[3.3 Block Diagram 14](#_Toc29452069)

[3.4 Use Case Diagram 14](#_Toc29452069)

[3.5 Activity Diagram 14](#_Toc29452069)

[3.5.1 Embedding Diagram 14](#_Toc29452069)

[3.5.1 Extraction Diagram 14](#_Toc29452069)

[3.6 Data Flow Diagram(DFD) 14](#_Toc29452069)

[CHAPTER 4: EPILOGUE 15](#_Toc29452070)

[4.1 Expected Output 15](#_Toc29452071)

[4.2 Work Schedule 15](#_Toc29452072)

[4.3 REFERENCES 16](#_Toc29452073)

# 

# LIST OF FIGURES

**FIGURE PAGE**

**3.3** Block Diagram: --------------------------------------------------------------------

**3.4** Use case Diagram: ----------------------------------------------------------------

**3.5.1** Activity Diagram (Embedding): -------------------------------------------------

**3.5.2** Activity Diagram (Extraction): --------------------------------------------------

**3.6** Data Flow Diagram:----------------------------------------------------------------

**LIST OF ABBREVIATIONS**

ASCII - American Standard Code for Information Interchange

CPU - Central Processing Unit

DBMS - Database Management System

LFCCs - Linear-prediction cepstral coefficients

LSB - Least Significant Bit

MD 5 - Message-Digest algorithm 5

MSB - Most Significant Bit

RAM - Random Access Memory

ROM - Read Only Memory

SQL - Structure Query Language

**CHAPTER 1: INTRODUCTION**

**1.1 Background**

Audio in Image Steganography is a desktop application. The purpose of this application is to provide the security for the confidential audio information. This application does not allow the hackers to view the data, can view only greyscale image file when it is being passed over the internet. Then at the recipient side the original information i.e., audio file will be extracted from the greyscale image by performing decryption operations in the encryption process each LSB (least significant byte) will be replaced by the encrypted data. During decryption process each data will be extracted from each LSB and then performs decryption operation which results into an original audio which was sent by the source side. The data is embedded into the greyscale image file. Before embedding it into the file, encryption operation will be performed by using the encryption key which is provided by the source. Then this greyscale image file will be passed over the net, even if hacker hacks it, can be able to see only a greyscale image file. At the destination side this data will be encrypted from greyscale image file and performs decryption to get original audio message.

**1.2 Problem Statement**

Cryptography is traditionally used mechanism for authentication of genuine users as well as for secure information. In traditional data communication system, there is no privacy of data. Data are transferred via insecure channel. So, any third person can easily track the information. In order to solve this problem our system is designed with high level encryption of data using the concept of steganography.

**1.3 Objectives**

1. To store audio information in more secure manner in system generated image.
2. To track audio information embedded in system generated image.

**1.4 Applications**

Audio in Image Steganography is an application developed for storing and tracking information inside and from system generated image. It helps to hide the audio information secretly inside system generated images. So, this software has many applications in various field like in any business company, military, museum etc. In military they have to send or receive information securely so the software can be beneficial. In museum there are historical images in the wall so, we can keep related audio information detailing the content of the given images in system generated images so a reader can simply get that information by scanning it.

**1.5 Project Features**

This system provides following features:

* High capacity encoding of data
* Audio steganography
* Secure store and transfer of information
* Easy tracking

**1.6 Feasibility Analysis**

The aim of the feasibility study was to analyze the strengths, weakness, opportunities, and threats of using this system as on possible solution for storing or hiding data more securely. It looked at the potential costs and benefits of using this system for this purpose and focused specifically on the energy sector.

**1.6.1 Economic Feasibility**

With such a low cost, this system is likely to appear many places – the low cost means that the software doesn’t have to create significant engagement to justify their existence. It doesn’t require a significant upfront or operational investment. It doesn’t require any expensive hardware to use this system, so this system is cost effective.

**1.6.2 Technical Feasibility**

Is this software technically feasible? Yes, it is. This system doesn’t need any expensive or powerful hardware to run or build. We have adequate technology available for the development of the system. User just need a pc to use this system.

**1.6.3 Operational Feasibility**

Talking about how this project will work in any organization or individual or how users feel about the system, it is easy to use and understand. With growing security concerns like cyber-crime, this system can be beneficial for all users it will provide security on data storing and transmission.

**1.7 System Requirement**

**1.7.1 Software Requirement**

* Python
* PyCharm
* Tkinter
* Visual studio code
* SQL, MySQL
* OS: Windows 10

**1.7.2 Hardware Requirement**

* Processor (CPU with 2 GHz frequency or above)
* Minimum 2 GB RAM
* Minimum 20 GB ROM

**1.7.3 Functional and Non-Functional Requirements**

**Functional Requirements**

Functional requirements are the requirements that that define specific behavior or function of the system.

* **Login:** Login function will authenticate the sender if username and password are correct Otherwise it will exit the system.
* Secret Audio Message File: In this file you will have to select the secret audio message.
* Image generator: The audio message is generating in image form where the audio message is hidden without losing its information.
* Sender: In this sender send the generator image to intended recipient.
* Receiver: In this receiver receives the generator image and opens in decryption option for getting hidden audio.

**Non-Functional Requirements**

Some of the Non-functional requirements of the project are as follows:

* Safety Requirements:

Sender and Receiver should make sure that only they are having the same software to encrypt and decrypt data inside image. Both should take care of eavesdropping.

* Security Requirements:

We are going to develop a software in which the message audio will be generate in image form. Only sender and receiver should be aware of encrypted message.

* Software Quality Attributes

The Quality of the software is maintained in such a way that only sender and receiver can communicate through image. There is no probability of knowing secret image.

**CHAPTER 2: LITERATURE STUDY**

Literature study is basically done to understand the concept of image generating form audio. Literature study suggest some algorithm which can be implemented to improve image processing, steganography and MD5 hashing.

**1.1 Research paper study**

**Paper 1:**

**Title of paper-**Information Security Based on Steganography & Cryptography Techniques: A Review

**Authors-**M. Tech Scholar Pramendra Kumar, Prof. Vijay Kumar Sharma

**Year of Publication-**October 2014

**Publishing Details-**RIET, Bhankrota, Jaipur, Rajasthan, India

**Summary**

In this research paper we understand the concept of Steganography & Cryptography. Cryptography is one of the classic techniques used for ensuring privacy of files and communication. It is the science of secret writing, converting messages or data into a different form to exchange messages between two parties who want the communication over an insecure channel. Steganography technique are closely related to cryptography to protect information from unwanted parties but the cryptography can offer two additional security services that are not offered by steganography at the moment, namely data integrity and non-repudiation. The steganography focuses on keeping the existence of the message as secret. It involves two major techniques: visual analysis and statistical analysis. Visual analysis tries to reveal the presence of hidden data through inspection, either with the naked eye (or ear in the case of sound) or with the assistance of a computer. Statistical analysis, on the other hand, attempts to reveal tiny alterations in carrier objects of statistical characteristics caused by steganographic embedding.

**Paper 2:**

**Title of paper-** Python Based Image Processing

**Authors-** Dr. Sanjay Shitole

**Publishing Details-** Usha Mittal Institute of Technology, SNDT Women’s University

**Summary**

In this paper we understand the concept of Python Image Processing Library. The Python Imaging Library, or PIL for short, is one of the core libraries for image manipulation in Python programming language. Many of the image processing tasks can be carried out using the PIL library such as image inversion, binary conversion, cropping, writing text on images, changing intensity, brightness, image filtering, such as blurring, contouring, smoothing and many more. PIL can be used for the image enhancement and the development of the Python based image processing application so that it becomes easy for the beginners to learn and understand the complex tasks of the image processing using Python based image processing.

**Paper 3:**

**Title of paper-** Hashing Algorithm: MD5

**Authors-** Shweta Mishra, Shikha Mishra, Nilesh Kumar

**Year of Publication-** September 2013

**Publishing Details-** Echelon Institute of Technology, Faridabad, India

**Summary**

In this paper we understood the concept of MD5 algorithm. The MD5 algorithm is designed to be quite fast on 32-bit machines. In addition, the MD5 algorithm does not require any large substitution tables; the algorithm can be coded quite compactly. MD5 algorithm takes as input a message of arbitrary length and produces as output a 128 bits message digest of the input. The authentication algorithm computes a digest of the entire data of the message, used for authentication. the message digest is registered with a trusted third-party, or encrypted via other means. The digest is used by the receiver to verify the contents of a message. It can also be used to encrypt the contents of a message, via a second pass over the data by another algorithm. MD5 requires that both the sender and receiver compute the digest of the entire body of a message.

**1.2** **Integrated Summary of Literature**

Before going deep into the steganography, image generation process and MD5 hashing, first and foremost, we need to understand the various components. The below list covers all the possible components that will be present.

**Message (Audio): -** refers to the part of the message which is intended to be hidden. This message will later be encrypted to make it even more difficult for anyone who tries to break the security to get hold of the hidden information message. This is the crucial component in a steganography message.

**Encryption Image: -** the audio message will be generating in an image form. That generated image will contain the audio message without losing the information.

**MD5 hashing: -** md5 hashing will be done in generated image to make an audio message more difficult for anyone who tries to break the security.

**CHAPTER 3: METHODOLOGY**

**3.1 Embedding Process:**

1. System start

2. Registered to the system if not registered.

3. Login to the system

4. Click on generate image button which redirect to image generation page.

5. Select audio

6. Select 'Yes' if you want to set password or select 'No'

7. Enter Password if 'Yes' selected

8. Select Proceed button

9 Create list with first value on list as '0'

8. Processing Password if it is entered

a. Hash input password using md5

b. Convert hashed password into decimal and finally in string

c. if length (password in string) ==38 concatenate extra bit '0' in left side

d. Each fetched value from string is converted in integer and appended into list.

9. If password is not set, append 39 0's on list.

10. Read binary of audio files

a. Convert binary of audio files into decimal using list

b. Append all the decimal files of audio in the same list where password was

stored.

11. Check the length of the list.

a. If remainder division of length of list doesn’t become 0 append 255 values till remainder becomes 0.

b. counts the added values

c. changes the first values of list as count values

12. Generate image

a. Height and Width for image is calculated by performing square root of output of length of list divisible by 3

b. Height and Width value is increased by 1

c. Fetch three values from list at each time

d. Fetched value is append as the value of Red Green and Blue Color.

e. Transparent value is kept as 255 as default

f. Pixel is putted according to coordinate system (X, Y) = (Height, Width)

13. Finally generated image is saved in the directory

**3.2 Extraction Process:**

1. System start

2. Registered to the system if not registered.

3. Login to the system

4. Select system generated image and start scanning

5. Check if password is set ask for password else continue

6. Hash the input password using md5.

7. convert hashed input password into decimal and finally in string.

8. Compare the input password with the scanned password.

9. If password matched scan all the pixel else stop showing error message

10. Remove all the extra bits added initially while generating the image

11. Finally generate the audio file and save it on the directory.

**3.3 Block Diagram**

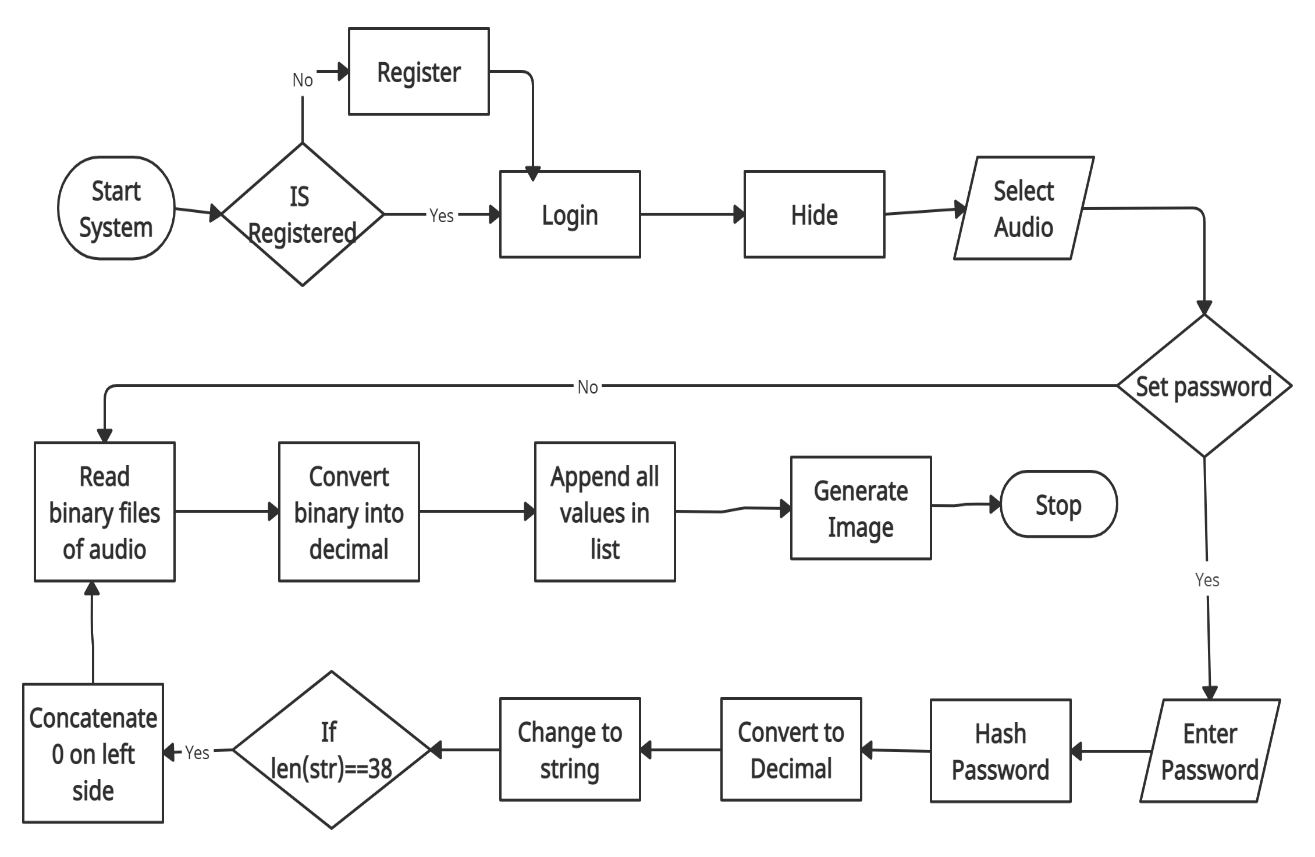
****

Fig: Embedding Process diagram

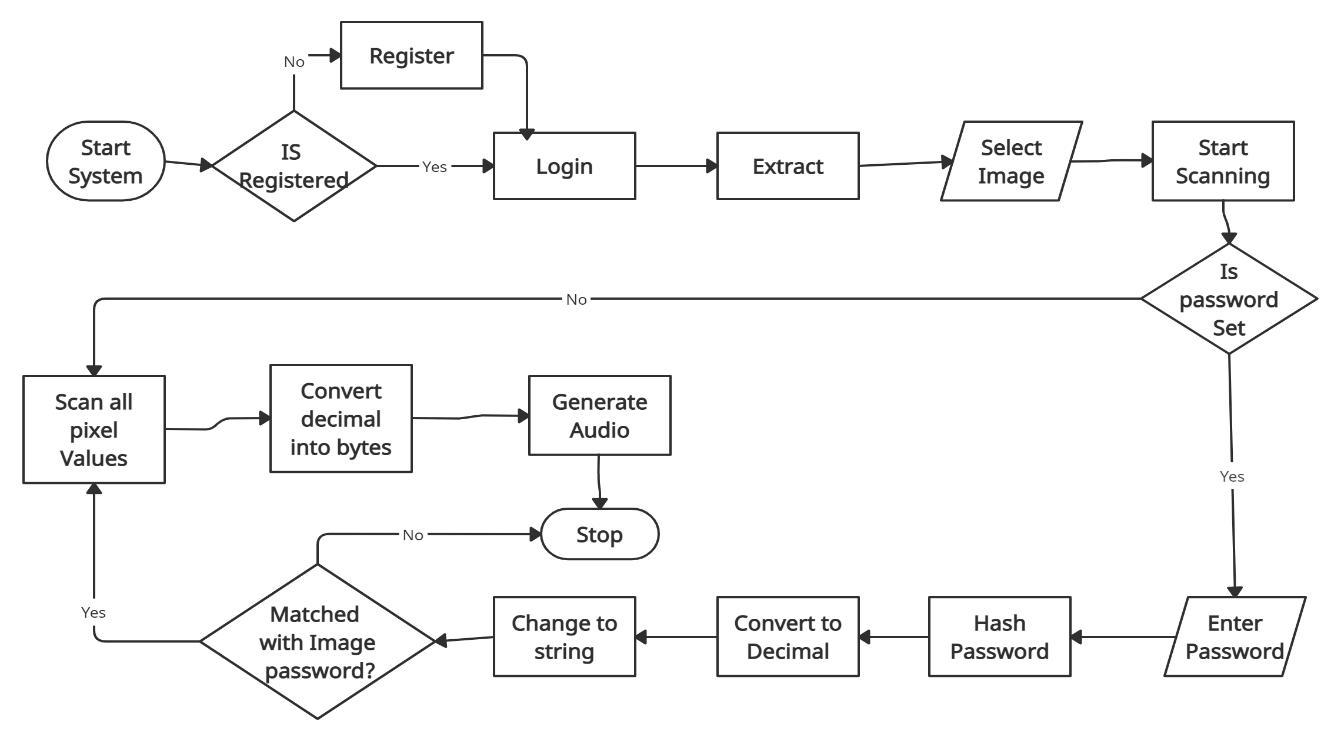
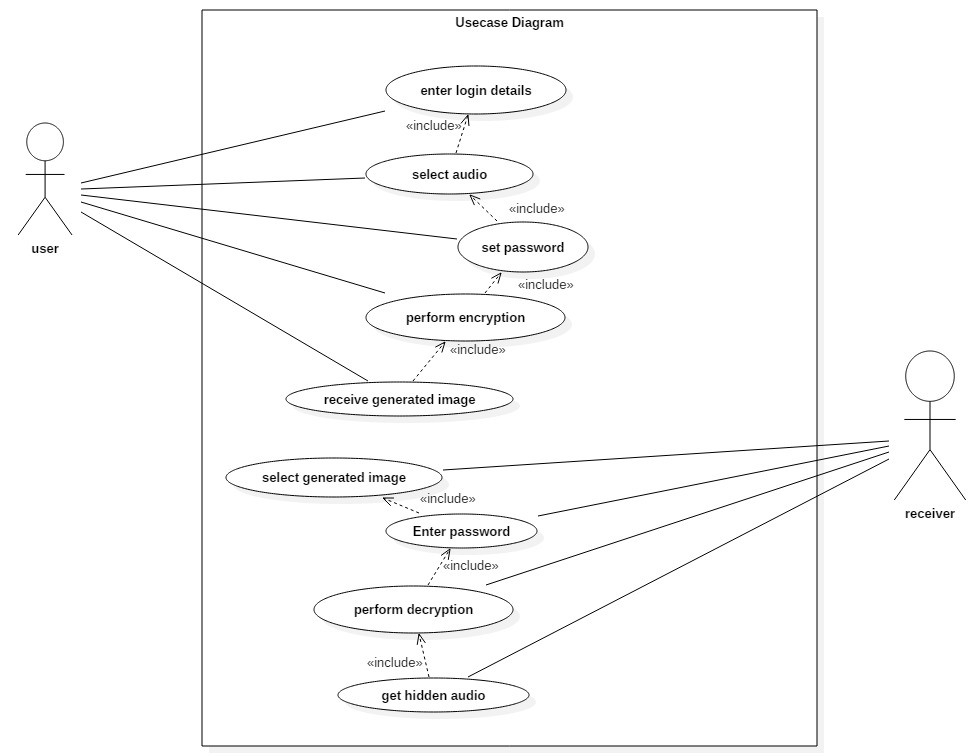


Fig: Extraction Process Diagram

**3.4 Use Case Diagram**

****

**3.5 Activity Diagram**

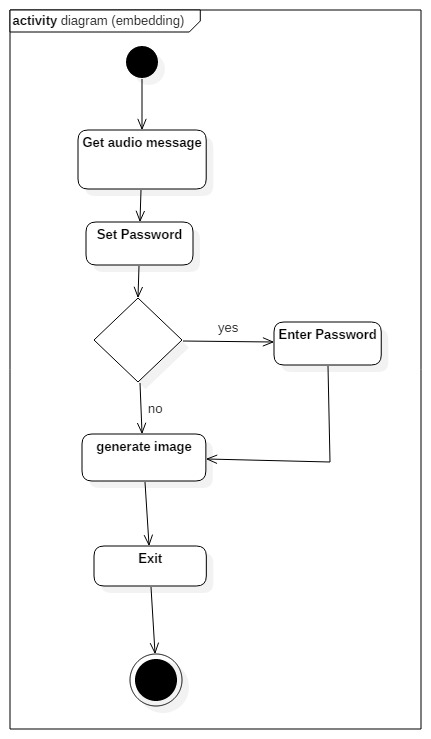


Figure: Embedding Diagram

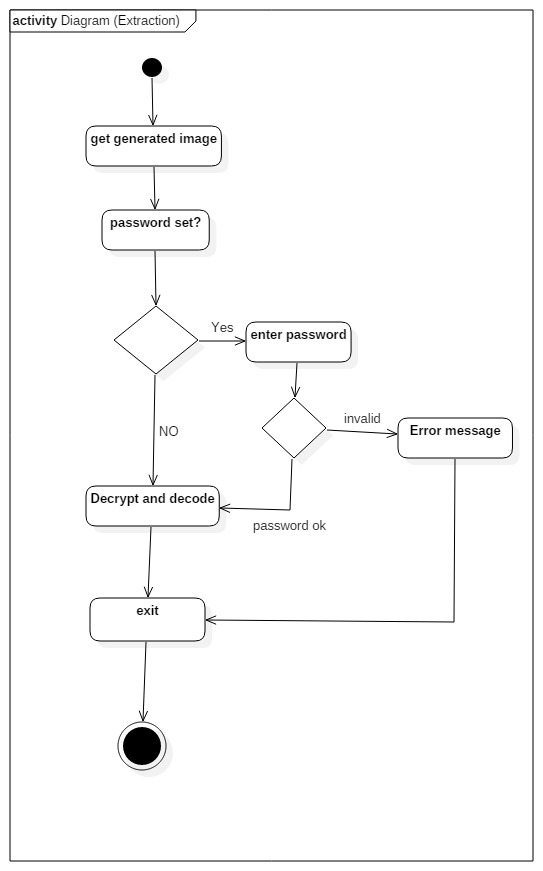


Figure: Extraction Diagram

**3.6 Data Flow Diagram**

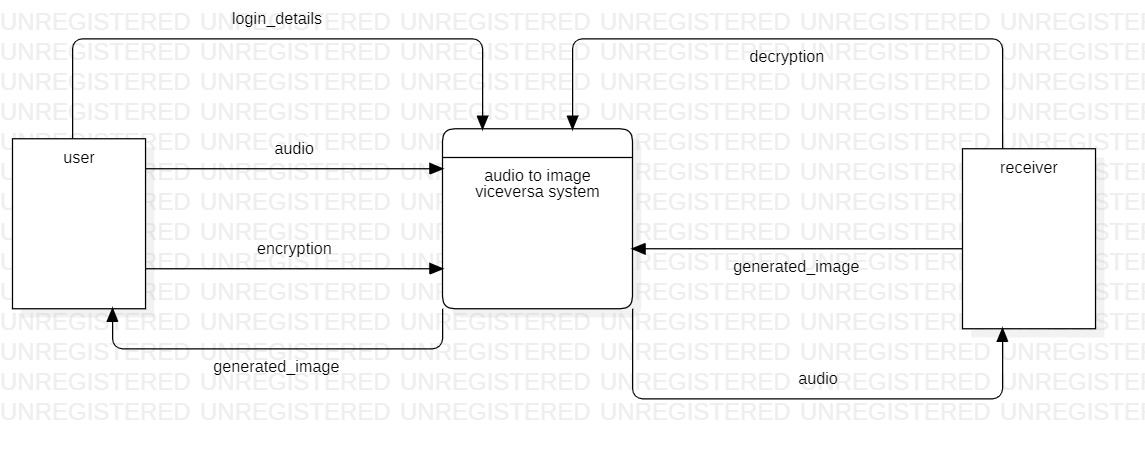
****

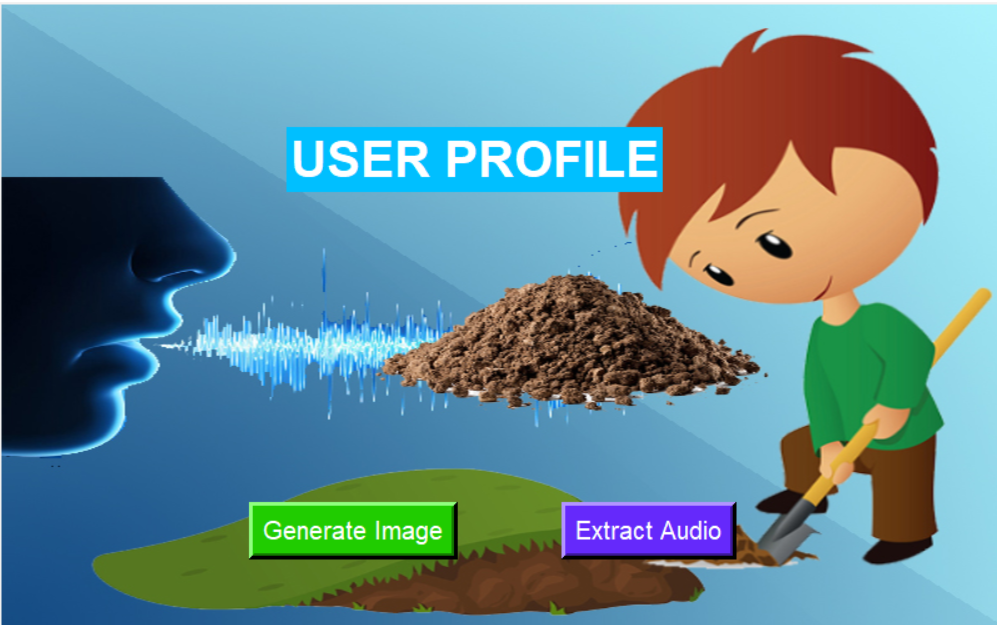
Figure: DFD Level 0

**CHAPTER 4: EPILOGUE**

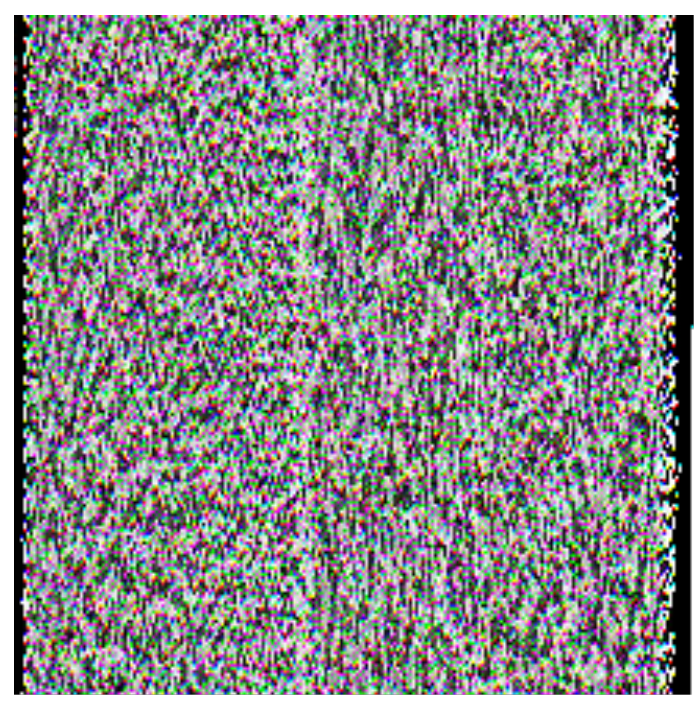
**4.1 Expected Output**

The target of this paper is to implement steganography techniques for confidential communication between two entities. This project hides the secret audio information by generating RGB image of secret audio information. Here we are using .WAV audio file format. By using raw data of audio information, we generate an RGB image. The generated image will contain the audio information without losing its information. The generated image is sent to destination with the help of private or public communication network. On the other side, receiver download the generated image using the software and retrieve the secret audio information.











**4.2 Work Schedule**

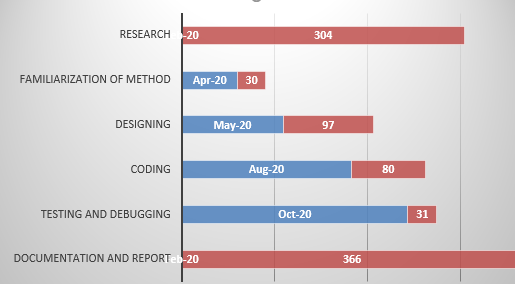


Figure: Gantt Chart

**4.2 References**

[1] M.ram mohan reddy s.s divya. Hiding text in audio using multiple LSB steganography and provide security using cryptography. International journal of scientic technology research, 1(6):68-70, 2012 shobha lokhande. 2012.

[2] Tanmay bhowmik pramatha nath basu. On embedding of audio in audio a case of steganography.ieee publication. Pages 203-206, 2010.

[4] Teoh suk kuan rosziati ibrahim.steganography algorithm to hide secret message inside an image computer technology and application, 2:102-108, 2011.

[5] Websites:

* <https://en.wikipedia.org/wiki/Steganography>
* <https://en.wikipedia.org/wiki/MD5>
* https://www.geeksforgeeks.org/image-based-steganography-using-python