Signature Text,Image and Audio Hiding in a Color Image using Steganography and Cryptography

Shivansh Bishen[1], Paurav Malik[2] , Saloni Rao[3] , Prakash Biswagar[4]

[1]Student, Dept of Electronics and Communication, R.V. College of Engineering, Bangalore, INDIA -560059
[2]Student, Dept of Electronics and Communication, R.V. College of Engineering, Bangalore, INDIA -560059
[3]Student, Dept of Electronics and Communication, R.V. College of Engineering, Bangalore, INDIA -560059

[4]Professor, Dept of Electronics and Communication, R.V. College of Engineering, Bangalore, INDIA -560059

[1]shivanshbishen.ec17@rvce.edu.in, [2]pauravmailk.ec16@rvce.edu.in, [3]salonirao.ec16@rvce.edu.in, [4]prakashbiswagar@rvce.edu.in

Abstract: Data Transmission in network security is one among the foremost vital issues in today's communication world. the end result of that's that Data security has gained an utmost importance because of the unprecedented increase within the data generated over the web, which could be a basic necessity of any application in information technology. The vigorous growth within the field of data communication has made information transmission much easier. But this kind of advancement has opened many possibilities of data being snooped. So, day-by-day maintaining of data security is becoming an inseparable a part of computing and communication. In this report, we've got explored techniques that blend cryptography and steganography together. Steganography may be a specialty of science to manage and conceal a chunk of important information inside image, audio, video or text documents. Steganography may be a method and study of composing a secret communication specified only the source and also the targeted beneficiary will realize the concealed information. the information concealed or covered process starts with the steganography method by identifying a network canopy and redundant parts, i.e. only permitted persons would be able to change without affecting the standard of that medium. The encoding method generates a Stego medium by substituting these redundant bits with concealed message content. In this report, various approaches for information hiding using both cryptography and steganography is proposed keeping in mind two considerations-size of the encrypted object and degree of security. Here, signature image, text , audio information is kept hidden into cover image using private key of sender and receiver, which extracts the data from stego image employing a public key. This approach are often used for message authentication, message integrity and non- repudiation purpose.

Keywords: **Steganography, Cryptography, redundant-bits**

1. INTRODUCTION

A huge amount of confidential data is transferred over the net rigorously. Today, plenty of interest is seen within the field of steganography and steganalysis. The first aim of steganography is to hide information in a very distributed media, so others cannot find it out. Cryptography and steganography are two sides of a coin, where cryptography uses encryption to form a meaningless message while steganography hides data existence. This technology is widely utilized in military surveillance, intelligence organizations, online races, web banking, clinical imaging, etc. the key message is hidden into a picture using steganography. The message is then transmitted to the receiver which extracts the hidden message from the stego image. The stego image must not even be discernible to the duvet image, that the intruder cannot locate any hidden message. the safety of the modification of the key data is obtained by two ways: encryption and steganography. a mix of encryption and steganography will be wont to enhance the info security. Steganography also can be used with cryptography, thus encrypted data is hidden into cover image, thereby generating a stego image. At the receiving end, data from stego image is retrieved employing a proper key. When a file is generated then some areas of the file may be substituted with the data which is required to be hidden, without seemingly changing the file or harming it. this allows an individual to hide information within the file and assure that no human involvement could notice the alteration within the file. The LSB method performs in an exceedingly superior way in image files which must have an inflated resolution and locate various colors. LSB method also performs well with audio files that have dissimilar sounds and an enhanced bit rate. The LSB procedure normally doesn't only facilitate the file size, but betting on the magnitude of the knowledge that's to be concealed inside the file, the file can become perceptively twisted.

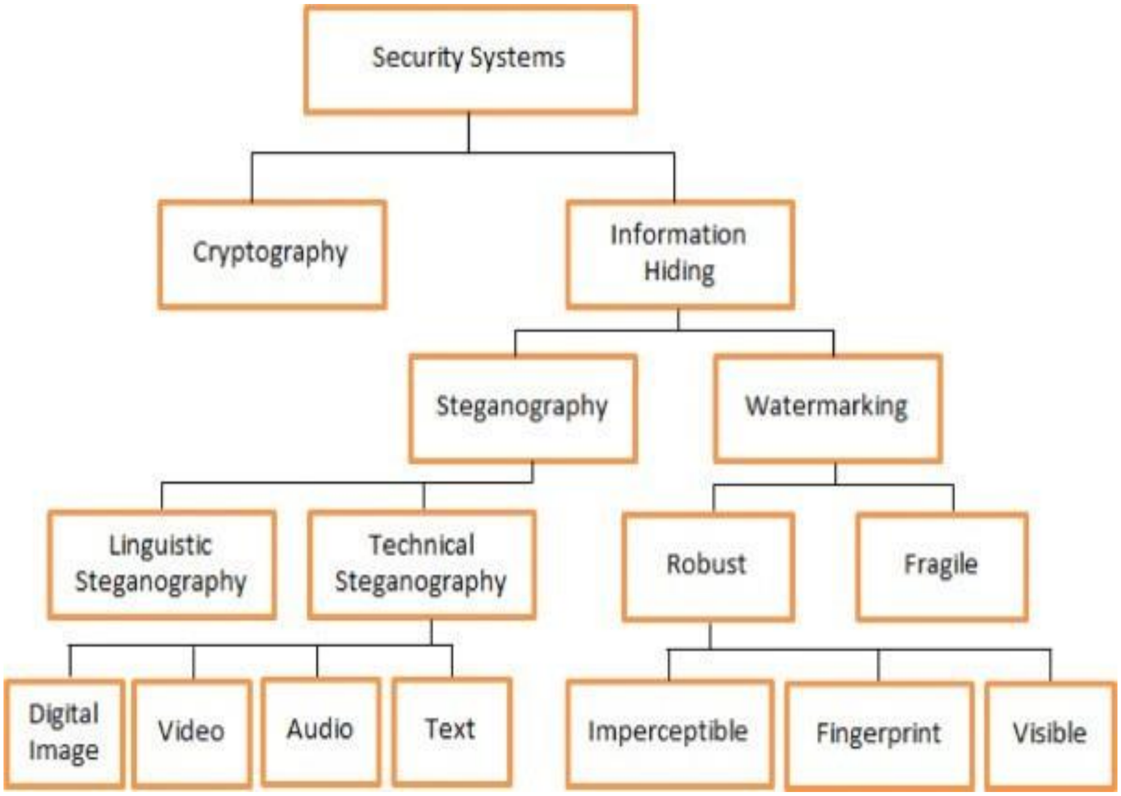


Figure 1 Security Systems

2. LITERATURE REVIEW

Data security has gained an utmost importance because of the unprecedented increase within the data generated over the web, which could be a basic necessity of any application in information technology. Here, signature image information is kept hidden into cover image using private key of sender and receiver, which extracts the knowledge from stego image employing a public key. This approach is used for message authentication, message integrity and non-repudiation purpose.

The paper [1] work deals with the study of interest within the fields of Steganography and Steganalysis with the image, audio or video stego media against the corresponding cover media (without the hidden information) and understand the method of embedding the knowledge and its detection. A two-layer protection is given to supply secured trans- mission. Here, RSA algorithm is employed for cryptography and LSB modification is employed for Steganography. In paper [2], an improved LSB Steganography which uses modulus function for data hiding method has been proposed and implemented which is best than previous methods in imperceptibility keeping the hiding capacity same. Whereas in paper [3], the system proposed during this study uses a canopy object, image specifically to cover the message to be sent. Before a message is embedded within the image, the message is first encrypted using RSA encryption algorithm.

The paper [4], discusses a few histogram cosine similarity matching method for real- time transport protocol (RTP) timestamp difference vectors and a clustering method of the world between the best-fit curves of two RTP timestamp difference sequences is presented. These 2 methods realize timestamp-based least significant bit (LSB) steganography detection respectively. Size constraint for Text File: To store 1-byte information (8 bits), a minimum of 8 pixels are needed for the quilt image. File should be a minimum of 8 times bigger (in terms of pixels) than the document.

The paper [5], proposes a way of image coding that hides the data along a particular pixel and on the subsequent value of the chosen pixel, that is, pixel + 1. One bit is hidden at the chosen pixel, and therefore the second bit is hidden on the pixel +1 value. In paper [6], the optimization techniques examined within the past, the performance of Genetic Algorithm (GA) based approaches are seen as a substandard technique compared to PSO based approaches with a target to enhance the performance of GA approach.

In paper [7], cryptography incorporated steganography is imply (CICS) to supply a highly secure steganography algorithm for the files of the multiple formats, The performance analysis of the tactic and therefore the measurement of the parameters like the PSNR and therefore the SSIM are done to confirm the efficiency of the proffered method. A digital signature is constructed upon the concept of public key encryption. a non-public key's operated to encrypt a hashed genre of the image.

3.BRIEF METHODOLOGY

- Generate Private and Public Key pair through RSA algorithm.
- Signature image information is being encrypted using Private Key of Sender
- At the sender end, encrypted signature header information is embedded at LSB of blue colour. Then the pixel information is embedded at LSB of the red colour of the cover image pixels. Thus the stego image is kept ready.
- At the receiver end, embedded information is retrieved from the stego image.

4.SPECIFIACTION OF DESIGN

Explanation of the techniques/methods used for text, image and audio hiding inside a cover image, the design follows the procedure, The secret text message in the proposed program is concealed within the cover image format. The hidden text in the cover image is concealed in the first phase, whereas the secret audio file is stored in the cover image file in the second phase.

Firstly, every text character and each cover picture pixel value is translated into binary. The Stego-key on the sender side is used as the password for embedding the hidden message in the cover picture format. Once the process of embedding the text file into the cover image is complete, an audio file is selected which is embed in same image file where the text file is inserted previously. The audio file in the WAV format is selected and embedded in the image file.

The resulting final or Stego-image is sent to the receiver through the desired channel of communication. While inserting the binary bit of secret text message into the conceal picture document. The every values of pixels in the cover image in decimal is converted into binary values and replaced using the LSB algorithm. Similarly, each value of the hidden text message is replaced by the cover images of LSB bit, this procedure is repeated until each text bits in image file are replaced.

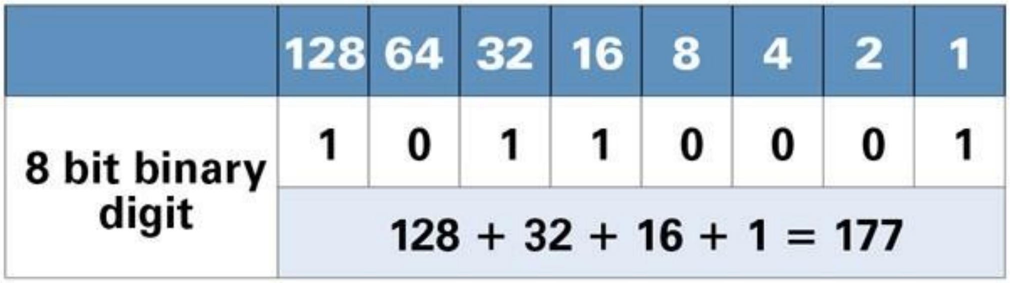
Similarly, the DCT (Discrete Cosine Transforms) technique is used to compress a hidden audio file. The audio samples will vary between -1 and + 1. When the samples are plotted in a graph, they are retrieving from the audio and transformed to digitized form and then embed into the shielded image file.

5. DIGITAL IMAGE

We can describe it as a finite set of digital values, called pixels. Pixels are the smallest individual element of an image, holding values that represent the brightness of a given color at a specific point. Hence, we can think of an image as a matrix (two-dimensional array) of pixels which contain a fixed number of rows and columns. Here, it is referenced to the raster graphic, which are basically dot matrix data structure, representing a grid of pixels, which in turn can be stored in image files with varying formats.

6. PIXEL CONCEPT

The intensity of each pixel is variable. In color imaging systems, a color is typically represented with three or four component intensities. Here, the project will be explained through the working of the RGB color model. The RGB color model is an additive color model in which Red, Green and Blue lights are added together in numerous ways to reproduce a broad array of colors. So each pixel from theimage is composed of three values (Red, Green, Blue) which are 8- bit values thatranges from 0 – 255.



	128	64	32	16	8	4	2	1
8 bit binary digit	1	0	1	1	0	0	0	1
	128 + 32 + 16 + 1 = 177							

FIGURE 2. 8-BIT REPRESENTATION

Every pixel has three values (RGB), each RGB value is 8-bit (this infers that it can store 8 binary values) and the rightmost bits are less substantial. Therefore, changing the rightmost bits will have a small visual impact on the final image. This is the steganography key to hide an image inside another by changing the less significant bits from an image and including the most significant bits from the other image.

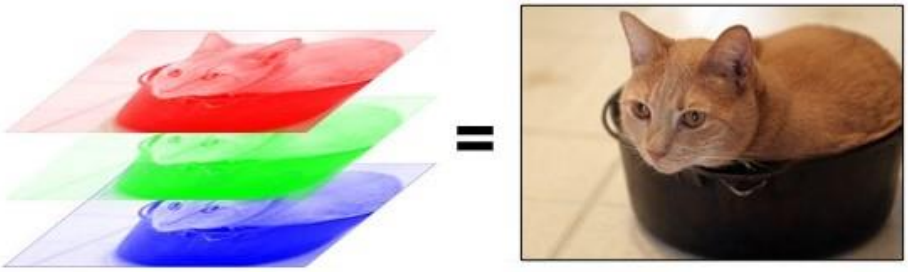


FIGURE 3. RGB COLOR MODEL

7.DESIGN METHEDOLOGY

7.1 Hiding Text and Audio Inside Image

- **Algorithm for Encoding**

(a) Step1: Read the cover image file

(b) Step 2: Perform edge detection of the cover image file chosen.

(c) Step 3: Remold the ASCII character or text message (P) into array form, then convert it into ASCII format (Q).

(d) Step 4: Remold the text message (P) into array form, then convert itinto ASCII format (Q).

(e) Step 5: Convert the ASCII message into a binary matrix.

(f) Step 6: Generate the key (k) encrypt the matrix using key P= (Q+K) Pi, where i =2; Perform the embed process with the LSB replacement algorithm. The result generated is Stego-image (Z).

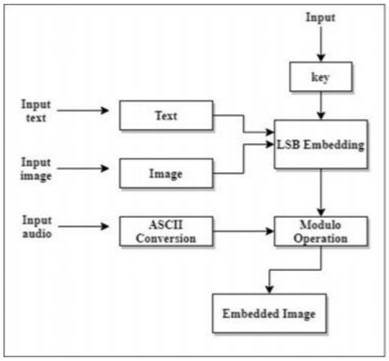


Figure 4. Encoding Process

(g) Step 7: An audio file (M) which is in WAV format is selected and each sample of audio is read and converted into matrix format as x (a, b).

(h) Step 8: The audio file read in the form of two-dimension matrix x (a, b).

(i) Step 9: The audio sample x (a, b) is embedded with the Stego-image (Z) that was previously obtained using LSB (Least Significant Bit) algorithm. Now, the final Stego-image with text and audio embedded in it is generated.

- **Algorithm for Decoding**

(a) Step1: The input in the decoding process is the Stegoimage (Z). Then, read the Stego-image and convert it into binary format.

(b) Step 2: In the receiver's side the image is multiplied with the inverse of the original matrix. i.e., a(x, y).

(c) Step 3: The decoded audio i.e. b(x, y) is not exactly equal to the original audio due to the image compression hiding i.e. DCT (Discrete cosine transformation) technique.

(d) Step 4: After decoding the audio file (M) using the reverse process of the LSB algorithm the next step is to decode the text message (p) from the Stego- image (z). Now, read the edge area along with the key to obtain the extraction matrix.

(e) Step 5: Decode the text message with the key to generate decode matrix P= (P-Q) Pi, where i=2.

(f) Step 6: Convert the decode matrix into ASCII form.

(g) Step 7: Remold and display the original text message

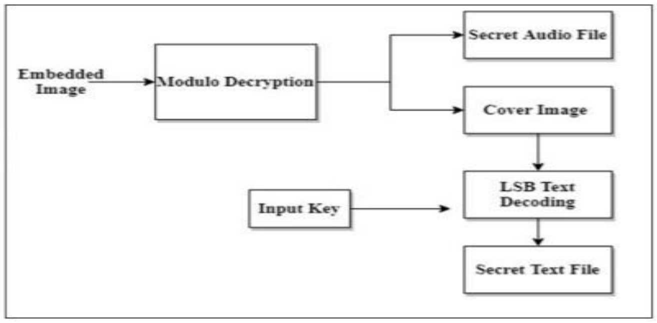


FIGURE 5. DECODING PROCESS

7.2 Hiding Image Inside Image

- **Algorithm for Encoding**

(a) Step 1: To hide an image inside another, the image which will be hidden needs to have at most the same size of the image which will hide it.

(b) Step 2: We must create two loops to go through all rows and columns from the images.

(c) Step 3: So, we get the RGB from the image 1 and image 2 as binary values

(d) Step 4 : We can usethe ”int to bin” method to convert a decimal value to a binary value.

(e) Step 5: We merge the most significant bits from the image 1 with the most significant bits from the image 2 Using the ” merge rgb” method

(f) Step 6: Finally, we convert the new binary value to a decimal value using the ”Z bin to int” method and after that set it to a new pixel position from the resulted image.

(g) Step 7: Now we have an image hidden inside another image.

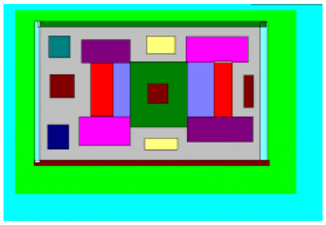


FIGURE 6. STEGO IMAGE WITH HIDDEN MESSAGE

- **Algorithm for Decoding**

(a) Step 1: To reveal an image, we must know how many bits were used to hide the image. In this case, we are using a fixed number of 4 bits.

(b) Step 2: First of all, we need to create two loops to go through all pixels from the image

(c) Step 3: So, we extract each RGB channel as a binary value from the current pixel Using the ” int to in” method

(d) Step 4 : Then, we create a new RGB value by concatenating only the 4 rightmost bits from the current pixel with zero values (to create a new 8-bit value).

(e) Step 5: . Finally, we convert the binary value to a decimal value and set it to the current pixel in the new image.

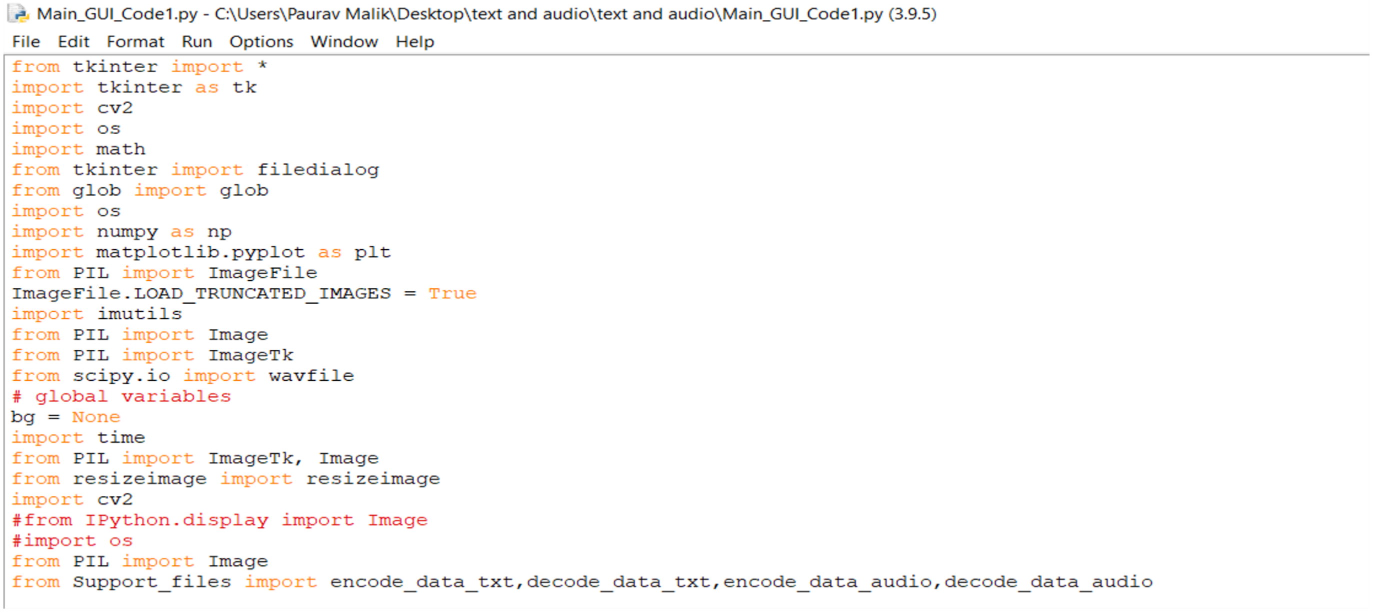
(f) Step 6: The developed algorithm has only one more last step to remove the black borders when the hidden image was smaller than the image which is hiding it.

(g) Step 7: Now we have the decoded message from the image.

8. IMPLEMENTATION OF USER INTERFACE

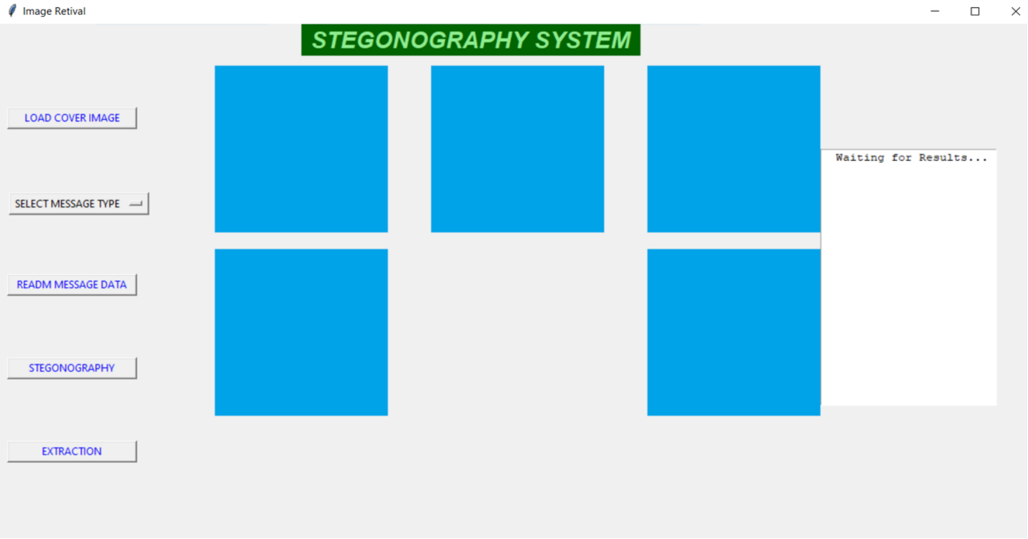
A step-wise implementation of our Steganorpahic encryption process to hide information in the LSB is as follows:

a. The user will start the application and run the code.
b. As soon as the code is run user has to import various libraries, Some Libraries are installed from external sources as It provides a Command Line Interface (CLI)to find, install, download and remove packages from PyPI and other Python Package indexes.After the libraries are installed the application starts up and a user interface is presented on the users screen as shown :
c. Now the given set of data or information, be it text, audio or image is taken, converted into ASCII values.
d. The user then imports the cover image and the input file that has chosen.
e. After the selection of the encryption of the information under the cover image begins.
f. Convert the disintegrated each ASCII in 4 value. Divide 8-bit number into 2-bit digit, which helps the user at the time of hiding the data.
g. Now the converted form of information is changed into an image format, mostly png. (lossless compression), which will be hidden under the cover image, whichwe are using for Steganography.
h. The converted and hidden image containing different form of information is then sent to receiver.
i. The receiver then starts the decryption of the sent image file.
j. Message input is extracted from the cover image.
k. The hidden message image is then decrypted and the information is extracted from the image in its original form.
l. This is how Steganography is done to hide different form of information under a 'Cover Image' using encryption and decryption algorithms.


Main_GUI_Code1.py - C:\Users\Paurav Malik\Desktop\text and audio\text and audio\Main_GUI_Code1.py (3.9.5)
File Edit Format Run Options Window Help

```
from tkinter import *
import tkinter as tk
import cv2
import os
import math
from tkinter import filedialog
from glob import glob
import os
import numpy as np
import matplotlib.pyplot as plt
from PIL import ImageFile
ImageFile.LOAD_TRUNCATED_IMAGES = True
import imutils
from PIL import Image
from PIL import ImageTk
from scipy.io import wavfile
# global variables
bg = None
import time
from PIL import ImageTk, Image
from resizeimage import resizeimage
import cv2
#from IPython.display import Image
#import os
from PIL import Image
from Support_files import encode_data_txt,decode_data_txt,encode_data_audio,decode_data_audio
```

FIGURE 7. IMPORTED LIBRARY



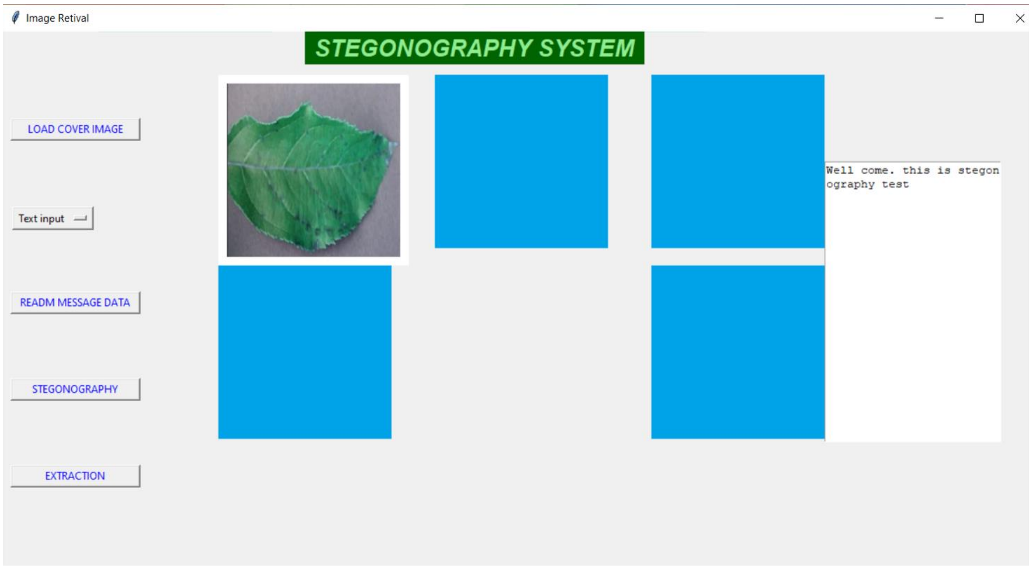
Waiting for Results...

FIGURE 8. CREATED USER INTERFACE

9. REQUIREMENTS OF THE INFORMATION

- For experimentation a coloured image of 512 X 512 is considered.
- Duration of the audio is less than 4 seconds.
- For the experiment of hiding the image inside another image we need to make sure that the image which is being hidden i.e. our data should be less than or equal to the cover image.

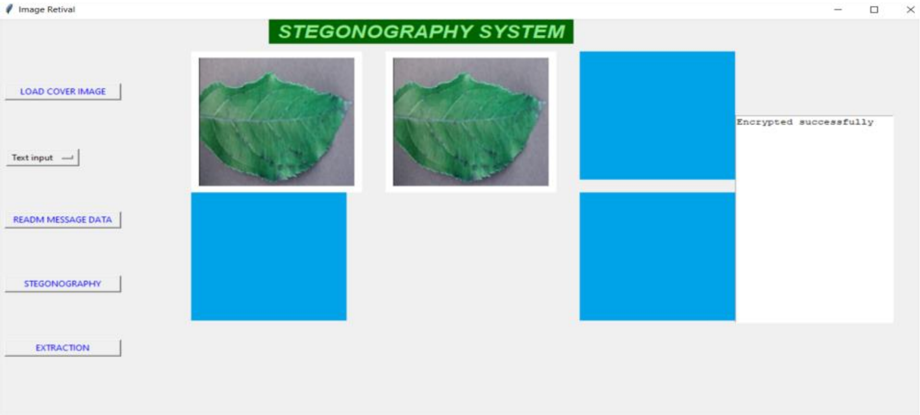
10. RESULTS FOR TEXT IN IMAGE ENCRYPTION



Well come. this is stegon
ography test

FIGURE 9. AFTER UPLOADING COVER IMAGE AND TEXT

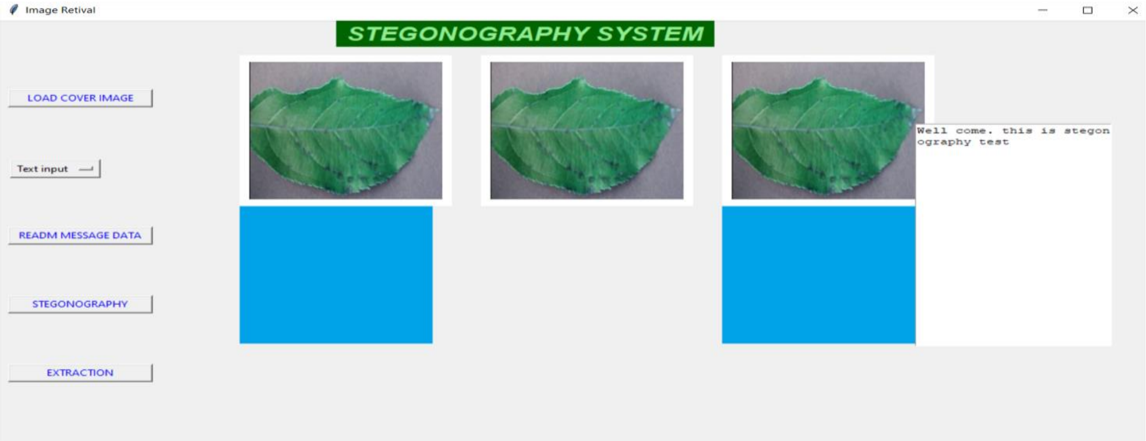
The above figure 9, we can see that the user has selected the input as Text input and has successfully loaded the cover image and the desired text file.



Encrypted successfully

FIGURE 10. SUCCESSFUL ENCRYPTION OF THE TEXT

The above figure 10, we can see that the text message has been successfully encrypted within the cover image using the encryption techniques.



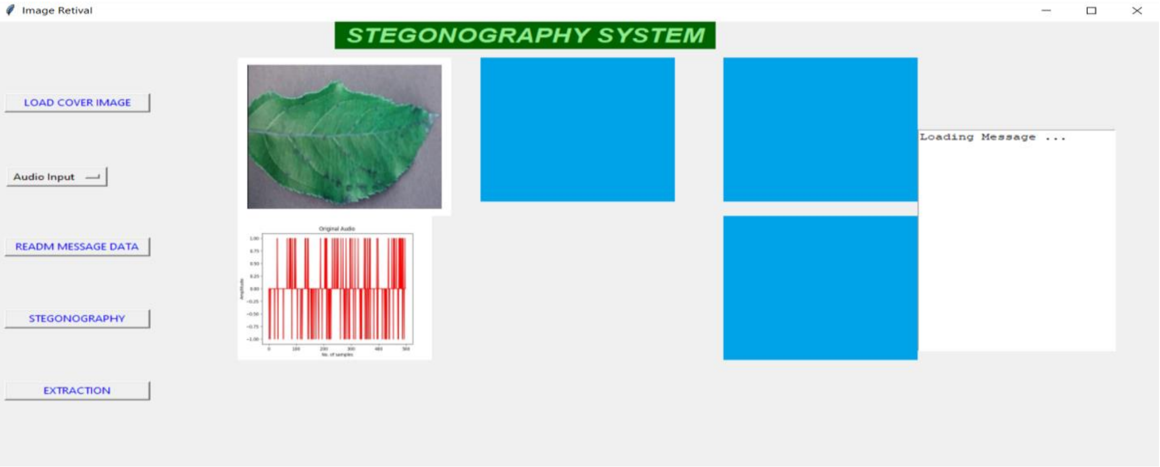
Well come. this is stegon
ography test

FIGURE 11. RETRIEVING OF TEXT

The above figure 11,we can see that the text message has been successfully decrypted at the receiver side. Having the same set of keys as the sender, the receiver gets the message out of the cover image.

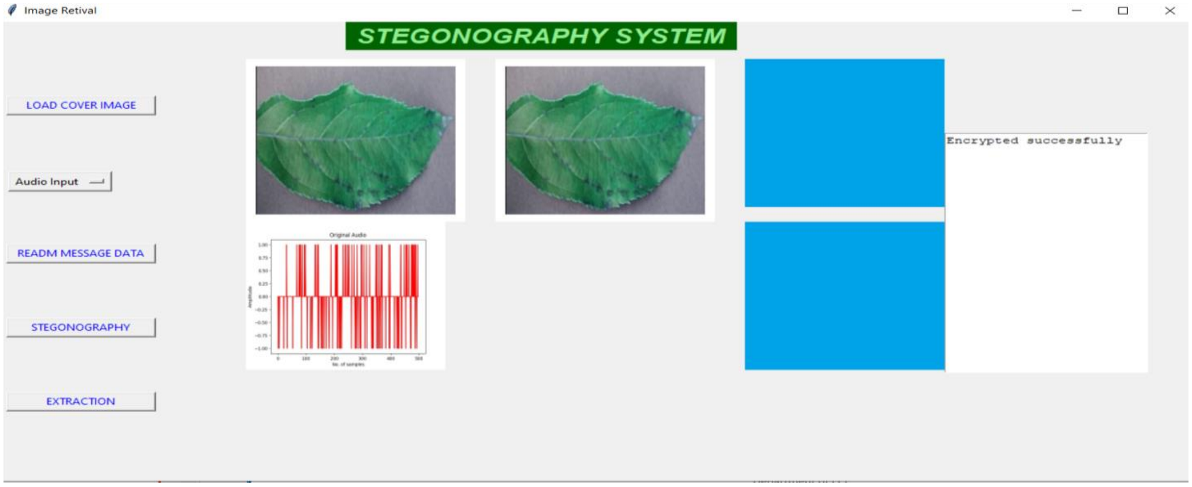
11.RESULTS FOR AUDIO HIDING INSIDE A COVER IMAGE

1. For Audio Encryption since we are using a 512x512 image some of our sampled audio values will come in negative.
2. Since we are loading a 512x512 image and we are getting both positive as well as negative values which make the data 16-bit .
3. But the image is of 8-bits so if we select a large audio file the image will not be able to store the audio and the encryption will fail.



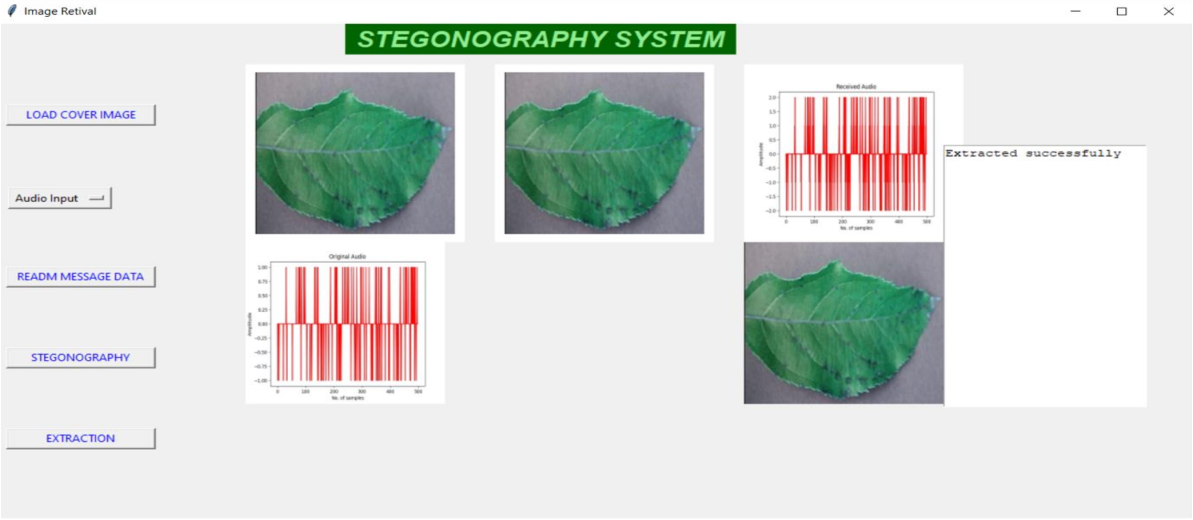
```
Loading Message ...
```

FIGURE 12. SELECTION OF AUDIO FILE AND COVER IMAGE



```
Encrypted successfully
```

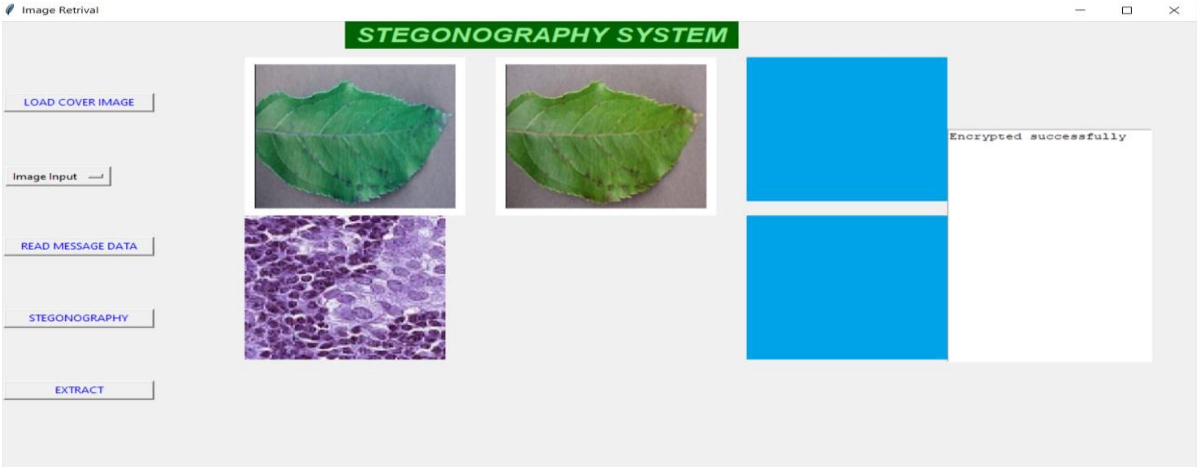
FIGURE 13. AUDIO FILE HIDDEN



```
Extracted successfully
```

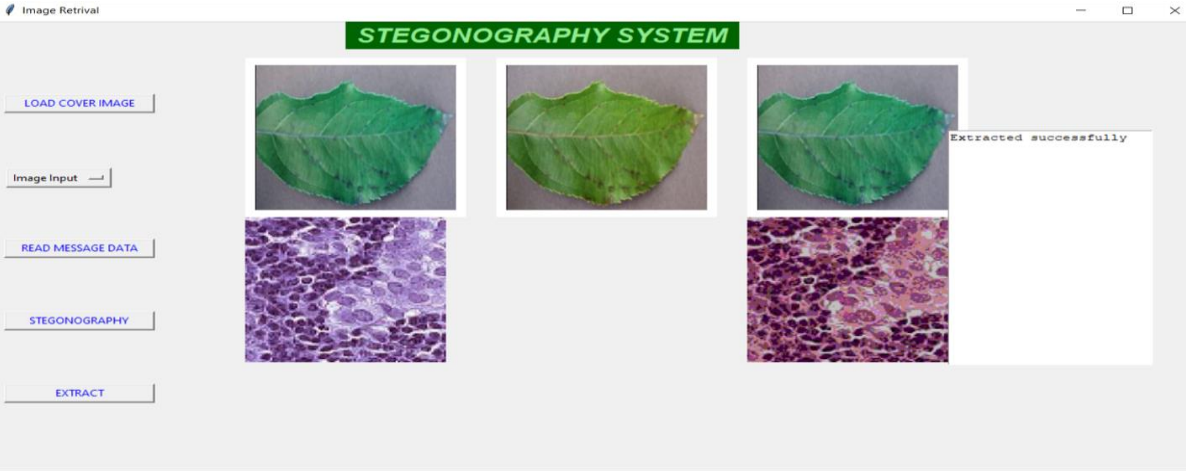
FIGURE 14.EXTRACTION OF AUDIO FILE

12. RESULTS FOR IMAGE IN IMAGE



```
Encrypted successfully
```

FIGURE 15.ENCRYPTED IMAGE IN IMAGE



```
Extracted successfully
```

FIGURE 16. DECRYPTED IMAGE FROM COVER IMAGE

13. CONCLUSION

The addition of security is a necessity these days and also a major challenge as every- thing is moving towards digital domain. Inclusion of security is a major challenge and an active area of research over the years. The project demonstrates the approach for hiding secret data inside a cover image which later can be extracted by the receiver.

Here we discuss, how steganography can be blended with the concept of digital sig- nature to provide a better support for improved secrecy and safety of datatransmission through the internet. The proposed secured communication of text, audio and image steganography using image steganography approach ensures safety of the text, audio and image. Here the text, audio and image files are converted into binary and encoded it into the cover file using bit-wise encoding.

LSB algorithm is preferred over the already existing wavelet transform method as it provides dual security and is faster than the conventional method. The work carried out provided us with efficient techniques for secure transmission of information.

13.REFERENCES

[1]A. B. A. Emad, A. G. H. Qahtan, and A. H. D. Jaafar, "Securing software defined network transactions using visual cryptography in steganography," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 8, no. 4, p. 2405, Dec. 2020. DOI: 10.21533/pen.v8i4.1737.

[2]A. Fatnassi, H. Gharsellaoui, and S. Bouamama, “A new hybrid steganalysis based approach for embedding image in audio and image cover media,” *IFAC-PapersOnLine*, vol. 49, no. 12, pp. 1809–1814, 2016. DOI: 10.1016/j.ifacol.2016.07.845.

[3]K. Joshi, S. Gill, and R. Yadav, “A new method of image steganography using 7th bit of a pixel as indicator by introducing the successive temporary pixel in the gray scale image,” *Journal of Computer Networks and Communications*, vol. 2018, pp. 1–10, Aug. 2018. DOI: 10.1155/2018/9475142.

[4]S. k Bandyopadhyay and S. Pramanik, “Application of steganography in symmet- ric key cryptography with genetic algorithm,” *INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY*, vol. 10, no. 7, pp. 1791–1799, Oct. 2013. DOI: 10.24297/ijct.v10i7.7027.

[5]R. Apau and C. Adomako, “Design of image steganography based on RSA algorithm and LSB insertion for android smartphones,” *International Journal of Computer Applications*, vol. 164, no. 1, pp. 13–22, Apr. 2017. DOI: 10.5120/ijca2017913557.

[6]V. R, “A SECURE STEGANOGRAPHY CREATION ALGORITHM FOR MULTIPLE FILE FORMATS,” *Journal of Innovative Image Processing*, vol. 1, no. 01, pp. 20–30, Oct. 2019. DOI: 10.36548/jiip.2019.1.003.

[7]A. A. AL-Shaaby and T. AlKharobi, “Cryptography and steganography: New ap- proach,” *Transactions on Networks and Communications*, vol. 5, no. 6, Dec. 2017. DOI: 10.14738/tnc.56.3914.

[8]W. Yang, S. Tang, and G. Wang, “RTP timestamp steganography detection method,” *IETE Technical Review*, vol. 35, no. sup1, pp. 59–67, Oct. 2018. DOI: 10.1080/ 02564602.2018.1536528.