

Secure End to End transmission using Audio Steganography and AES encryption

MSc Academic
Cyber Security

Anurag Chandrabali Gautam

Student ID: x18145060

School of Computing
National College of Ireland

Supervisor: Prof. Imran Khan

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Anurag Chandrabali Gautam
Student ID: x18145060
Programme: MSc in Cyber Security **Year:** 2019- 2020
Module: Academic Internship
Supervisor: Mr. Imran Khan
Submission Due Date: 12/12/2019

Project Title: Secure End to End transmission using Audio Steganography and AES encryption.

Word Count: 6399 **Page Count** 19 pages

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature:

Date: 12th December 2019

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission , to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project , both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Secure End to End transmission using Audio Steganography and AES encryption

Anurag Chandrabali Gautam

X18145060

Abstract

Steganography refers to data or a document hidden in a digital image, video or audio file. If a person perceives the files in which the data is stored inside, there will be no evidence that any information is concealed. So the person is not going to try to decrypt the data. Mostly, LSB encoding is used to encode the text in the image which is called as Image steganography. But image steganography is susceptible to pixel degrading techniques which allows attacker to degrade the image pixels and recover the secret message. This prototype will act as the secondary secure channel of transmission, when the key of AES encryption is compromised. In this paper, we have implemented the 256-bit AES encryption and image and audio steganography using LSB encoding and DWT. Audio files are less susceptible to attack. We also study the audio steganography with the cryptography method to accomplish the safety.

Keywords: 256-bit AES encryption, LSB encoding, DWT, Audio Steganography.

1. Introduction

The speedy evolution of science and technology in the telecommunication will create new ways for some people to exploit as hackers, crackers, phreakers, and so on to endanger information security. It will cause in damages if the data is on the erroneous side. The protection of classified data is something that must be addressed. For these data transmission professionals, data sharing and transfer of confidential data have been an ever-present concern in today's information age. From the beyond times to the existing instances to preserve the personal facts steady has continually been a first-rate difficulty. Researchers always determined it interesting growing stable strategies such that the information should attain from the sender to without revealing it to any third party. Hence, many methods are developed to transfer data securely. The most used methods used to overpower this threat are Steganography and Cryptography.

Cryptography is defined as the conversion of the secret message text into the incomprehensible ciphertext. The various aspects of Cryptography in securing the information are,

- a) Confidentiality: Only a certified person can read the transmitted data.
- b) Authentication: The identity of the source of the message is known properly.
- c) Non- Repudiation: This requires that the communication cannot be refused by either the recipient or the receiver of the message.
- d) Integrity: The modification on the transmitted and stored data is only certified to the authorized person.
- e) Access Control: Requires that access may be managed through the target system.

- f) Availability: Whenever an authorized person needed resources, the computer system resources must be available.

Steganography is known as the process of inserting digital data into another digital medium such as textual content, photos, audio, or video signals, without exposing its existence inside the medium. If a person views the item in which the statistics are hidden inside, there will be no evidence that any information is concealed. So the individual won't try to decrypt the data. Steganography is further divided into Audio Steganography, Video Steganography, and Image Steganography. Both these methods provide some safety of facts. Neither of them alone is steady enough for sharing information over an insecure communication channel and is prone to intruder attacks. Although those strategies are regularly combined to reap better tiers of protection but nonetheless there is a need for a noticeably secure device to transfer records over any communication media minimizing the risk of the intrusion.

There are many types of approaches to perform a successful steganography such as Least significant bit (LSB), DWT (Discrete wavelength Transform), Dual Key Approach, Multi-Level Clustering (MLC). LSB (Least Significant Bit) is one of the classical methods commonly used for steganography audio. Many researchers have been interested in developing it because of its simplicity. DWT (Discrete Wavelength Transform) is primarily based on the steganography approaches the wavelength coefficients of the obscure photos are modified to embed the secret message. In the recent past, a DWT-based algorithm for hiding image data has been proposed that embeds the secret message in the cover image band of Channel.

How image steganography and 256-bit AES encryption is combined with audio steganography is used to provide additional and better security for an end to end transmission.

There are few cons of image steganography, which is it can be compromised using pixel degrading technique, and it may lead to revealing the secret message or the confidential text inserted in the cover image file. Therefore, I came up with the new technique for inserting and transmitting secret messages securely from the sender to the receiver. Firstly, we will use 256-bit AES encryption to encrypt the secret text message, we all know that AES encryption is unbreakable, but when the key of the AES encryption is compromised or in future the AES encryption fails to secure the secret message, we will use our technique to transfer secret message from end to end. In our proposed techniques, we will encrypt the secret message with AES encryption, and we will encrypt it in the image file which would be the cover image for the secret message by using LSB encoding and later we will use another type of steganography to secure the stegoimage which is audio steganography. We will use LSB encoding to insert the stegoimage into the audio file, which will act as the cover for the stegoimage. For extraction of the message by the receiver, the receiver will use LSB decoding or LSB extraction method twice, and it will come up with the ciphertext of the secret message, and later, AES decryption can be used to decrypt the ciphertext into the plaintext or secret message.

2. Literature Review

In this part, it features an outline of the literature introducing applications on which the audio steganography is used to overcome in the case of failure of the encryption and the image steganography. Steganography is used on a substantial scale in the field of hiding the data in some cover files. There are many existing techniques that use the various types of steganography and cryptography and techniques to secure the transmission.

2.1 Least Significant Bit (LSB)

Steganography of the Least Significant Bit (LSB) is one of those techniques in which the least significant portion of the image is replaced by data bit. According to Rini Indrayani (2017) [1], MP3 is compliant with ISO MPEG-1 Layer 3, where FF FA or FF Fb bytes mark the header. For each frame, audio data was started on the 37th byte, aligned with ISO 11172-3. On each of them, the header is allocated from the first byte to the fourth, while the fifth to the 36th byte was the part of side data. To avoid altering the basic structure of the used MP3 file, the bits of the secret message would change only by the bits of audio information. A message insertion method is the least significant bit by modifying the first byte of audio information to be a secret binary message representation that will be concealed later. So you can add a bit of a secret message on any audio information. Original audio information, as shown in the figure 1, is the secret messages embedded in the letter A 01100101's alphabetical shape. The insertion of this binary interpretation is shown in the figure 2 in the original audio data. In each last bit, there is a switch that is substituted by a binary interpretation of letter A. The size of the MP3 cover and secret message, however, has an absolute impact on the test execution of the altered LSB method. The larger the size of the MP3 cover and the smaller size of the secret message, the fewer noise and vice-versa, the smaller the size of the MP3 cover, and the bigger the size of the secret message, the additional noise will be produced.

According to K. Thangadurai (2014) [2], to attain the better security, they have built image established steganography beside in conjunction with cryptography techniques. In the paper, the author has conveyed the difference between the cryptography and steganography, and it has conveyed that how strong cryptography and steganography combined are. Author has stated various algorithms for insertion of secret message in Grayscale Image using Least Significant bit.

Algorithm for inserting text message in Grayscale Image is,

Step 1: Read secret text message and the cover image, which is to be concealed in the cover grayscale image.

Step 2: Conversion of the secret text message into the binary bits.

Step 3: Calculating the LSB of each pixel of the cover image.

Step 4: Each bit of the secret text message will be substituted with the Least Significant bit of the cover image one by one.

Step 5: Writing Stegoimage.

Algorithm for retrieving secret text message from Grayscale Image is,

Step 1: Reading the Stegoimage.

Step 2: Calculating the Least Significant Bit of each pixel of the stegoimage.

Step 3: Retrieving the bits & converting each of 8 bits into character.

Author concludes that using the least significant bit for insertion of the secret message in the cover image is straightforward, but the secret message can be certainly decoded.

According to Sahib Khan (2015) [3], concealing data in the edges might enhance the excellence of the stegoimage substantially. In this paper, the author has used the spatial domain

data hiding technique for hiding the secret message in the true edges by replacing the 4 least significant bits of cover image. Hiding a secret message only in true edges reduces the hiding ability a little but hiding information in true edges pixels prevents changes in histogram nearly to zero and histogram variations and results in stegoimage of high quality. The author has proposed the edge detection technique which has following steps:

1. Pre-processing: By using the Gaussian low pass filter, we will remove the noise from the cover image.
2. Calculating gradients: The gradient's magnitudes and directions are calculated at each point of the image. The area where the gradient is high is labelled as edges, whereas a small gradient means non-edges.
3. Double Thresholding: Double thresholding is used to the consequence of the non-maxima containment, to establish the potential edges.
4. Data Hiding: Finally by replacing edge pixels with the 4 least significant bit, data concealing of the secret message takes place.

The results gained indicate that the technique suggested hides large amounts of secret data with better visual image quality in the cover image compared to other methods.

According to Chandni Arun (2017) [4], the method used to refer to the model is the LSB XOR method of substitution, while it enhances the use of protection. It is among the other functions, one of the most suitable and simplest methods. It is a way of hiding data that is used for the purposes of security. This paper is also enclosed to give a brief idea through an algorithm using the method of encryption and decryption that shows the recovery in security. Here we have a random 8-bit secret key that initially XOR with the RGB colours leading to data sharing embedding and then we get extracted information after replacing the pixel LSB which is a genuine message from the encoding process. It can hide a vast number of elements compared to the present data hiding and data revealing applications. It leads to the LSB method's distortion reduction and improves performance without disturbing the hidden information. For payload capacity and temperature tolerance, the LSB approach is retained, whereas the adjustment of the pixel value is responsible for high safety.

2.2 Discrete Wavelength Transform (DWT)

According to Vinita Korgaonkar (2014) [5], it offers a novel method to hiding video text information. Using frequency domain coefficient of structures, video steganography is brought. Authors method incorporates a Discrete Cosine Transform (DCT) and Discrete Wavelength Transform (DWT) technique to conceal information in order to obtain more PSNR and a high hiding power ratio. DWT and DCT convert a digital image into frequency domain measurements from a spatial intensity domain. 2D DWT transforms a digital image into four sub-bands providing details of estimate, perpendicular, parallel and transverse. Sub-bands LL, LH, HL and HH are decomposed using the low-pass filter and high-pass filter image. The LL sub-band is an original image's low-frequency band and thus its look is more like the original image. The embedding phase, video of any extension, is taken as an input to hide inside secret data. Here video functions as a cover media divided into several frames from which non-key frames are selected for the purpose of inserting. Then each frame is transformed into the space template of YCbCr colour. Transformations of DWT and DCT were applied to Y, Cb and Cr. For embedding, the high frequency sub-band is used. Consider only non-key frames for secret data embedding. For extraction phase, Stego video will be read to take away the video's secret message. Stego video is divided into several frames that are used to extract non-key frames. Then each frame is

converted to a model of YCbCr color space. The transformation of DWT and DCT is applied to Y, Cb and Cr. To obtain bits from DWT-DCT coefficients of Y, Cb and Cr, high frequency sub-bands are used. Binary bits are converted into a char that is read in a text file.

According to Sunil Kumar Yadav (2017) [6], using 2-DWT, SVD and FFT steganography method for hiding data. The result is calculated based on the PSNR, SNR, WPSNR and MSE to determine photo value for recommended technique for better conclusion. The transformation of the Wavelength is generated by repeated filtering of the measurements of the image on a row by row and column by column basis. A 2-DWT image decomposition involves quite a combination of band details reminiscent of LL frequency estimate band, perpendicular element band HL frequency, parallel information band LH frequency, and disproportionate transverse element band high frequency. DWT is used at the small computational cost to achieve just the right picture retrieval base. FFT is a DFT set of rules which decrease the form of computations wished for N elements from $2N^2$ to, in which $2N\log N$ is the bottom-2 algorithm. Because DFT and IDFT essentially require the same type of computations, our analysis of DFT's effective computational algorithms also applies to the IDFT's efficient computing. SVD sever through $m \times n$ real matrix A, correct in three matrices $A = USVT$ in which U and VT are $m \times n$, $n \times n$ orthogonal patterns. S is the transverse matrix of $n \times n$. The S elements on the transverse are the most convenient nonzero and are well-known as A's SVs. The approaches to watermarking are defined as follows. The assessment of success is measured on many parameters. The results of the simulation confirm that this approach holds a fine image of excellent quality. It is important in the assessment of exceptional IP operations.

According to Sabyasachi Kamila (2015) [7], the approach suggested hides covert bits in three higher frequency components to ensure that the effect of embedding on the cover image is negligible and not focused in the sensitivity domain. The method works on the frequency domain by employing 2D Haar DWT on the cover image to embed hidden bits in the higher occurrence elements of the cover image. Three ways method was followed to enforce the security. A decimal array of hidden bits is created at first. Secondly, a dynamic block is built that incorporates values from three different higher frequency components and finally bits are inserted in some selected block parts. To measure the distortion value of the image, PSNR value is calculated of the embedded image. The product of this approach shows a strong stegoimage visual quality with desirable characteristics of steganalysis resistant.

According to Vijay Kumar (2010) [8], the effect on the performance of stegano images in terms such as PSNR by embedding the secret message in different bands such as CH, CV and CD. The author has performed 6 different attacks. The cover image is divided into four sub-images as approximation coefficients (CA), horizontal detail coefficients (CH), vertical detail coefficients (CV) and diagonal detail coefficients (CD) in this method. Similarly, the hidden image is broken down into four sub-images. Both sub-images are separated into frames that are not overlapping. The blocks of the cover image approximation coefficients are subtracted from the hidden image approximation coefficient. These coefficients' differences are referred to as error blocks. The best matched CH block is used to replace an error block. The result of this experiment shows that the substitute of the error block with transverse information coefficients (CD) gives PSNR better than other coefficients.

2.3 Multi- Level Clustering (MLC) Algorithm

According to Sachin Jangid (2017) [9], Multi-Level Clustering is used to improve the performance of video steganography, Multi-Level Clustering algorithm uses K-Mean clustering

for frame cover clustering. Transform the Cover Video Frame and Secret Image to the groups in this process. Now some chosen group will use LBP(Local Binary Pattern) technique to insert the Secret message.

Following are the steps for embedding secret data:

- Step 1: Converting the Obscure Video into the Frames.
- Step 2: Converting the Obscure video Frames in RGB.
- Step 3: Use the Cover Video Frames method of K Mean Clustering and divide the video frames into clusters.
- Step 4: Select Number of clusters in which secret message will hide.
- Step 5: Insert the LBP methodology secret message.
- Step 6: Get the frames that are based on steganography.
- Step 7: Convert video from these images.

Following are the steps for extracting the secret data:

- Step 1: Convert the image of steganography into various frames.
- Step 2: Converting the RGB Frames to Space Lab colour.
- Step 3: In Stego Video Frames, apply K Mean Clustering.
- Step 4: Extracting the message from the cluster frames selected using LBP.

3. Research Methodology

The subsequent part gives an outline of the methodology utilized in the proposed prototype for securely transmitting secret message from one end to the another. The key concept is to build the secure channel for transmission of data when the AES encryption is compromised or the cover stegoimage is compromised using the pixel degradation method. In future, when AES encryption will be compromise, this will act as a secure channel to transmit secret data from sender to receiver. Therefore, the proposed method uses the 256-bit AES encryption, Image Steganography using LSB encoding technique and Audio Steganography using DWT technique. The secret message which is to be send to the receiver will be encrypted using 256-bit AES encryption then it will be encoded into a image file using LSB encoding method as image steganography is vulnerable to pixel degrading method, we have implemented the additional security for it which is encoding stegoimage into the random audio file and transmit to the receiver. By using Discrete wavelength transform (DWT), we will encode stegoimage into the audio.

3.1 Comparison of Cryptography and Steganography

Cryptography	Steganography
The encrypted letter could be seen by anyone, but cryptography make the message not understandable.	Steganography is hiding the message in another median so that nobody will notice the message.
The result in cryptography is the cipher text.	The result of information hiding is the stego-media.
The goal of a secure cryptographic is to prevent an interceptor from gaining any information about the plaintext from the intercepted cipher text.	The goal of secure steganographic methods is to prevent an observant intermediary from even obtaining knowledge of the mere presence of the secret data.
Any person has the ability of detecting and modifying the encrypted message.	The hidden message is imperceptible to anyone.
Steganography cannot be used to adapt the robustness of cryptographic system.	Steganography can be used in conjunction with cryptography by hiding an encrypted message.

Table 1: Comparison between Cryptography and Steganography

3.2 Comparison of Image steganography and Audio steganography

From the following table 2 & 3, we can see the difference between the various techniques of the image and audio steganography. Image steganography has 3 different techniques incorporate with their advantages and disadvantages. Where, audio steganography has 6 different techniques incorporate with their advantages and disadvantages as shown in the table 3.

Steganography Techniques	Cover Media	Embedding Techniques	Advantages
Image Hiding	Image		
LSB (Least Significant Bit)		This method is used the least significant bit of every pixel in one image to hide the most significant bit to another	Simplest & easiest way of hiding information.
DCT (Discrete Cosine Transform)		Embeds the information by altering the transformed DCT coefficient	Hide data can be distributed more evenly over the whole image in such a way to make it robust.
DWT (Discrete Wavelength Transform)		This technique works by talking many wavelets to encode a whole image	Coefficient of wavelet are altered with the noise within tolerable level.

Table 2: Different techniques of Image Steganography

Methods	Weakness	Firmness	Data hiding technique
LSB	Easy to extract	Simple and easy to hide information	LSB of each sample at audio is embedded by a bit of hidden information.
Echo hiding	Low security of information and low capacity	Without the problem of additive noise	Hiding information with introducing echo at cover signal
Balance coding	Easy to extract	More powerful than LSB	Change LSB of balance bit of samples
Discrete wavelet transform domain	Data recovery with losing	To make the high embedding capacity and clarity	Changing wavelet coefficient to hiding information
Spread spectrum	More bandwidth occupation	Best firmness and increasing the clarity	Spread information under all signal frequencies
Phase coding	Low capacity	Stable against signal processing options	To fluctuate the phase of cover signal.

Table 3: Different Techniques of Audio Steganography.

3.3 Advance Encryption System (AES)

Encryption is essential for the security of the internet today. Using mathematical computations, an encryption system scrambles sensitive data to convert data into code. Only with the accurate key can the original data be uncovered, granting it to remain safe from all but the permitted parties. Encryption is used by firms of all sizes across all areas to encrypt their data.

Organizations need to conceal passwords, personal identification information, and private messages from the despicable groups. That's when the AES comes in. AES has been developed to meet the needs of the U.S. government. Federal agencies relied as their encryption algorithm on the Data Encryption Standard (DES) in 1977. DES has been designed by IBM with a 56-bit symmetric-key block cipher design and has continued used effectively for nearly 20 years. It was clear by the 1990s that DES was not extensively safe enough. Today, AES is a reliable and widely adopted system. For programming languages like python, C++, C, Java, Javascript, AES libraries have been created.

How Does 256-bit AES work?

AES uses symmetric key to provide cipher. This ensures that the same secret key is used for both encryption and decryption, and a copy of the key is required by both the sender and recipient. The benefit of symmetric systems such as AES is its speed. Since a symmetric key system needs less computational capacity than an asymmetric one, running is quicker and more efficient. AES uses the encryption rounds that execute the transformation of the cipher. Typically, each round consists of some developing blocks built to create a function together, which is then operate several times. The number of rounds performed by AES varies on the size of the key at 128 bits, 10 at 192 bit–12 and 256 bit–14. [10]

Every round of the AES encryption contains of four levels:

- a) **Confusion is provided by the Sub-bytes** – Confusion is a thing of a secure cipher function as it conveys to AES. It builds the connection as complicated as possible between the ciphertext and the symmetric key. This generates non-linear tables that eliminate repetitions extremely well.
- b) **Diffusion is provided by Shift rows** – Diffusion is an additional thing of the secure AES cipher function. The aim here is to disintegrate the plaintext arithmetical structure over the ciphertext by supplying that portion of the input to each portion of the output.
- c) **Further diffusion is provided by Mix Columns for added effectiveness.**
- d) **Mixing of the key is done by Add_Round_Key**, Unable an attacker to determine what the cipher does. [11]

Ironically, there is no Mix Columns layer in the last round. It makes the system of encryption and decryption symmetrical.

How safe 256-bit AES is?

Successful brute-force attack on 265-bit AES could not be carried out, and any such effort would need approximately as many permutations as 1,100 supported by 75 zeroes. But Dutch researchers were able to recover 256-bit AES encryption keys in 2017 using a side-channel attack with enhanced antenna processing and signal processing. [11]

3.4 Least Significant Bit (LSB)

Least Significant Bit (LSB) encoding is the simplest way to insert secret data into the cover file such as text, audio, video, photo. The secret data can be hidden in the speech by substituting the least weighting value of a sampled speech signal with binary bits of secret data. The only purpose in the receiver is to retrieve bits of secret messages from the appropriate locations. A pseudorandom system can be used to monitor the place in which the hidden binary bits will be stored to increase the exposure complexity of secret data. [12]

Algorithm for embedding the secret message in the color image is,

Step 1: Read the image pixels and store them in an image-array.

Step 2: Converting the secret message which is to be embedded into the binary message.

Step 3: Read this binary bit into a message array.

Step 4: Select the pixel from the image-array and select from the message array the characters and place them in the Least Significant Bit of the pixel.

Step 5: The image obtained will be an embedded image containing hidden information. [2]

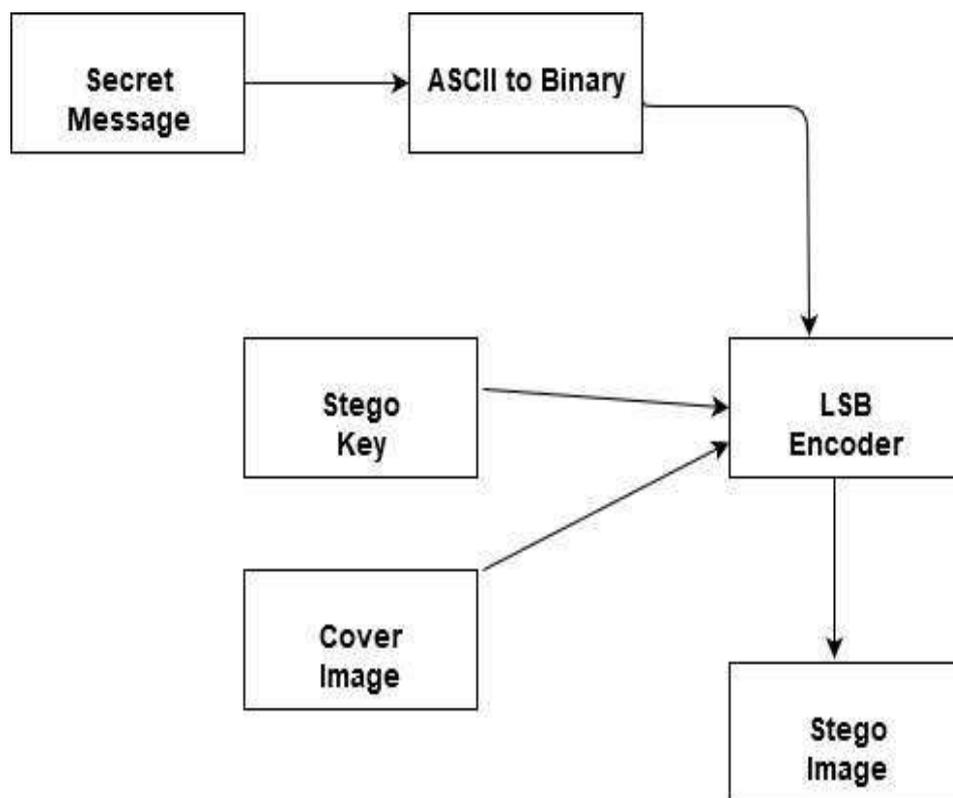


Figure 1: Insertion steps in LSB Encoding

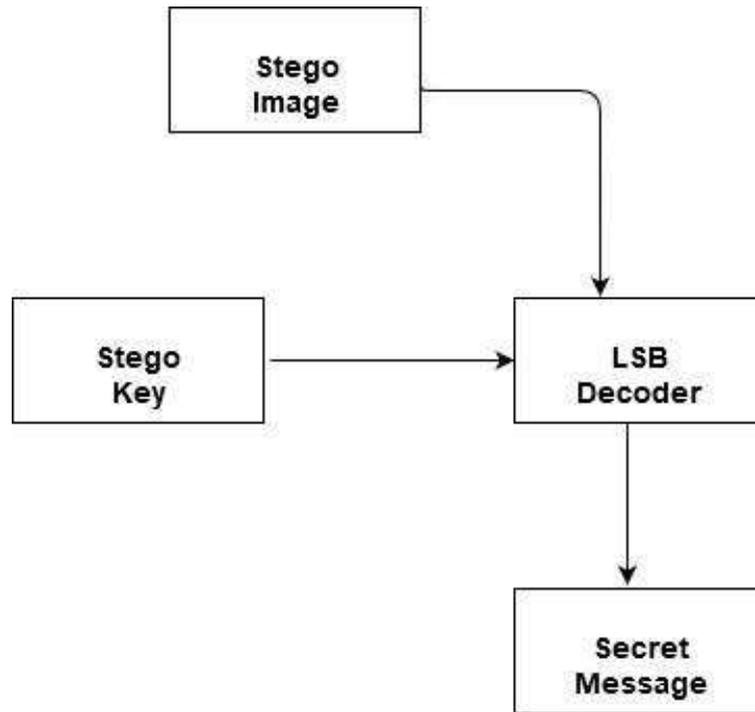


Figure 2: Extraction method in LSB Encoding.

3.5 Discrete Wavelength Transform (DWT)

The discrete wavelet transformation (DWT), as proposed by Daubechies in 1988 and others in the late 1980s, has encouraged broad research into how this transformation could be used to analyze time series. One emphasis of this work was on the adaptability of the wavelet the wavelet variation breaks down a time-series change and thus generates variance analysis (ANOVA). [13]

The transformation of the Wavelet is created by repeated filtering of the image measurements on a row by row and column by column foundation. DWT converts a digital image into frequency domain measurements from a spatial intensity domain. 2DDWT converts a digital picture into four sub-bands providing details of the calculation, perpendicular, parallel, and transverse. The LL, LH, HL and HH sub-bands are disintegrated using the low-pass filter and high-pass filter image. The LL sub-band is a low frequency band of an original image, and therefore, its appearance is more like the original image. [5]

4. Design Specification

The proposed system has been developed and introduced, which provides to be safe from the steganalysis attack such as pixel degradation, and in case the AES encryption key is compromised. Also, it has tried to secure the secret message salting and used the PBKDF2 algorithm for better security, which will prevent the Brute force attack. The proposed prototype is categorized into two phases: Embedding Process and Extraction Process.

4.1 Embedding Process.

Embedding process of the prototype can be defined as the whole insertion process of the image file in the cover audio file. From the below figure, we can see that the process starts with choosing the confidential, secret message for the process. That secret message is encrypted using the 256-bit AES encryption and salting as well. The whole rounds of encryption process of the AES give the ciphertext as a result. Then the Ciphertext of the secret message is embedding into the cover image file by using LSB encoding. LSB encoding method embeds the binary bits of the ciphertext into the least weighted bits of the cover image file. LSB encoding provides us a

new image that is encoded with the ciphertext. Later stegoimage is used as the file, which is to be embedded in the cover audio file by using Discrete Wavelength Transform. Discrete wavelength transform is used because it encodes the binary bits of the image file with the high-frequency bits of the audio file and results in the steganographic audio file, which is embedded with the image file.

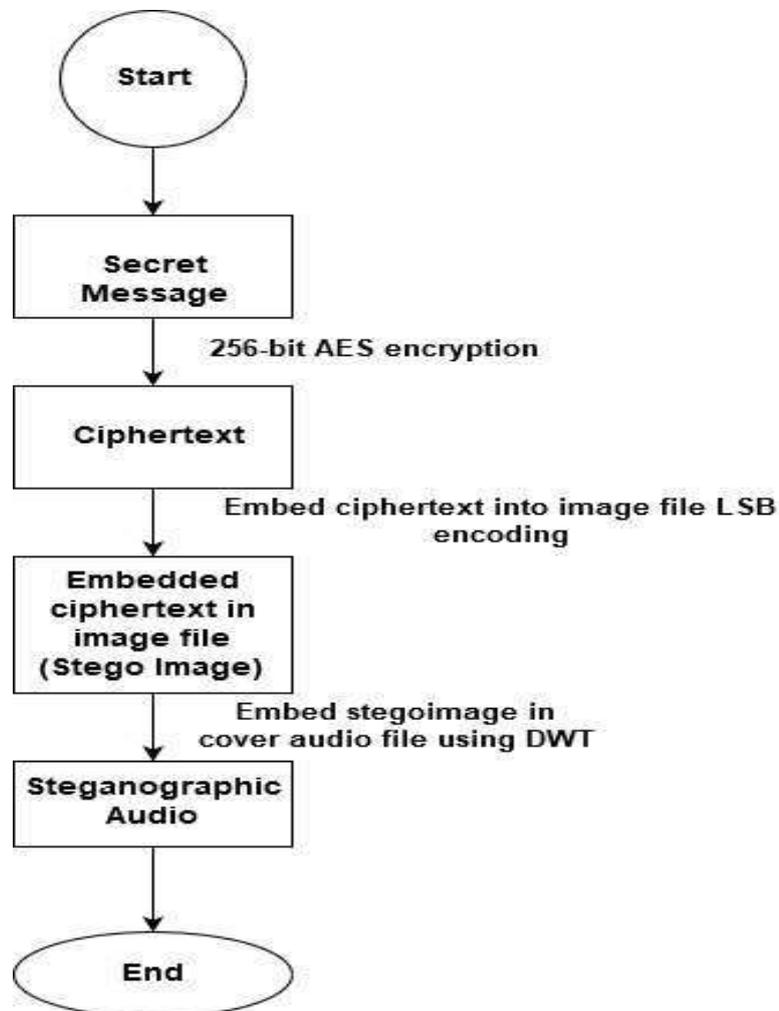


Figure 3: Embedding process of the proposed system.

4.2 Extraction Process.

Extraction Process of the prototype is similar to the embedding process but in a reverse manner as we can see it in the below figure. The extraction process starts with the choosing steganographic audio file which is to be recovered. By Discrete wavelength transform, we will extract the embedded stegoimage file, which is called as a recovered image. Then that recovered image will be used for the extraction. By using LSB decoding, the embedded ciphertext is extracted from the stegoimage. Then AES decryption is used to decrypt the ciphertext with the same key, which was used to encrypt it, and the key also present in the stegoimage with the ciphertext. This gives us back the secret message.

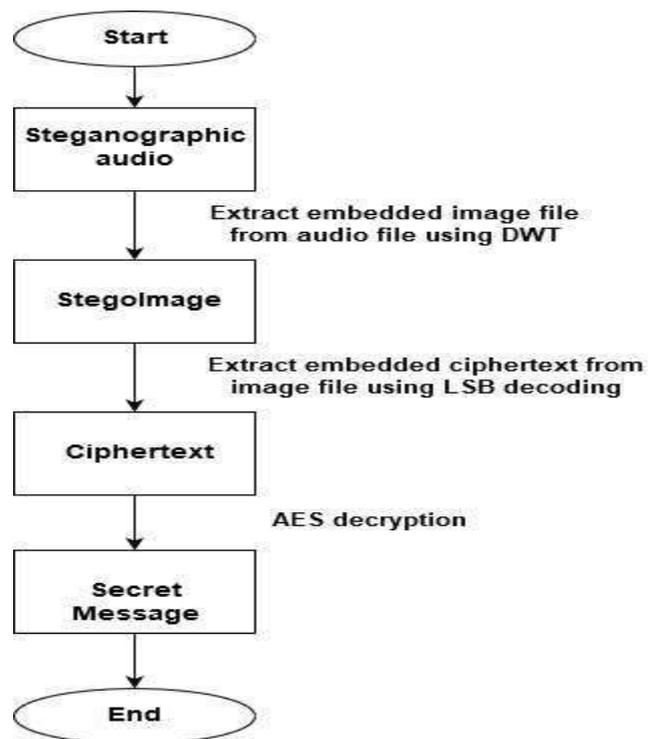


Figure 4: Extraction process of the proposed system.

5. Implementation

In this research, the proposed system, which is demonstrated by implementing the encryption and decryption code on the terminal of Linux OS, which uses python 3.8 and MATLAB application, is used for further implementation of the embedding code.

We have created the python script for AES encryption and decryption, which includes importing of the in.txt file, which contains a secret message, and we will export the ciphertext.txt file, which contains ciphertext of the secret message.

```

root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# python AES.py --password pass123 --salt 1234 --infile in.txt --outfile ciphertext.txt --encrypt
  
```

Figure 5: Encryption command in Linux

The following figure 6. shows the ciphertext of the secret message, which was imported in the python script.

```

a2hsJRxTmFEtmkTJzg\QucaPFVZ96GJI nM7H/LUUKPk=
  
```

Figure 6: Ciphertext of the secret message.

The exported ciphertext of the secret message was embedded using the MATLAB code for the image steganography. By embedding the ciphertext, we have created an original image and the stegoimage of the covered image, which contains ciphertext. We have used goku.png file as a cover image file, and we get originaliamge.png and stegoimage.png file.

A discrete wavelength transform is used to embed the stegoimage file into the cover audio file. When we extract the stegoimage from the audio file by using Discrete Wavelength Transform, we get a recovered image as shown in the figure 7. We can analyse with the human visual that

original image and the recovered image are not same, there are some bit loss while extracting the image from audio.

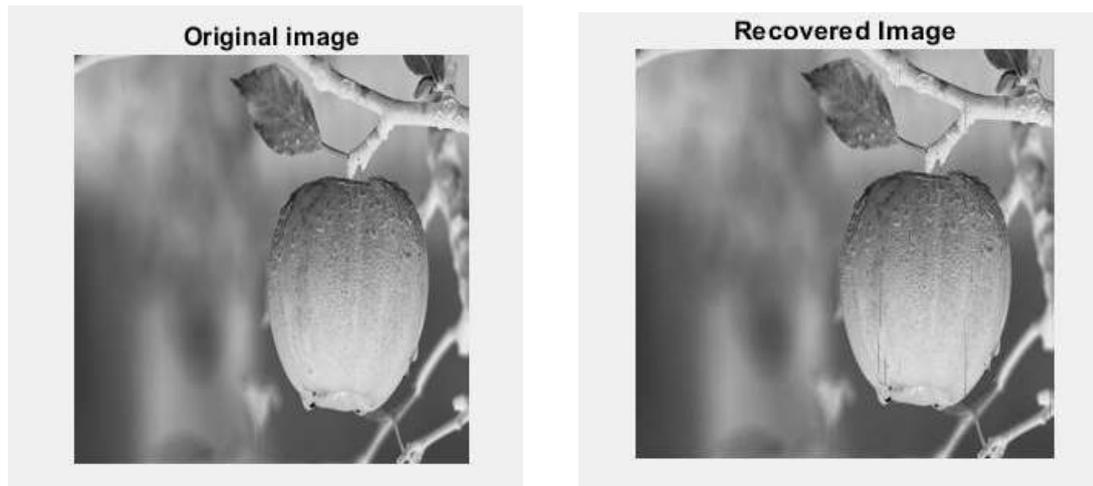


Figure 7: Original Stegoimage and Recovered Image from the cover audio file

PSNR: 89.9935 MSE: 6.5122e-05 Bit errors : 7

PSNR measures the peak signal to noise ratio between the two images in decibels. This ratio of two images is used to measure the quality between original image and compressed image. The higher the PSNR value, the quality of the recovered image will be better.

MSE (Mean-Square Error) can be represented as the cumulative squared error between the recovered and original image. The value of the MSE must be lower it represents the lower error rate.

For recovering the ciphertext from the recovered image we will use LSB decoding. After recovering the ciphertext from the recovered image we will decrypt it using the AES decryption but, in our case, as we can see in the figure 8, due to loss in the bits, we couldn't able to retrieve the proper ciphertext which was encoded in the image.

```
| a2hsJ  
|
```

Figure 8: Recovered Ciphertext from the recovered image.

6. Evaluation

We have performed following 3 attacks on the 3 different images and calculated the PSNR value and MSE value of those image after attack. [14]

Attack	Original Image	Recovered Image	PSNR	MSE	Bit error rates
Filtering			89.9935	6.5122e-05	7
Noise Addition			64.9452	0.0208	14743
Resampling			57.6292	0.1122	24650
Filtering			82.6489	3.5334e-04	14
Noise Addition			64.8654	0.0212	16318
Resampling			55.5489	0.1812	78446

Attacks	Original Image	Reconstructed Image	PSNR	MSE	Bit error rates
Filtering			89.4041	7.4589e-05	29
Noise Addition			64.9213	0.0209	31489
Resampling			57.5763	0.1136	56569

6.1 Discussion

We have performed the filtering, noise addition and resampling attack on the 3 images which were apple.png, goku.png and lena.png and we have found the recovered image with their PSNR value, MSE value and Bit error rate.

6.1.1 Filtering

Filtering with 1 tab average filter gives us complete recovered image same as the original image in three of the images with the highest PSNR which means it has the better quality of image while recovering and the lower MSE rate which indicate the lower error rates of the recovered image.

6.1.2 Noise Addition

Noise addition attack gives us entire recovered image same as the original image in three of the images with the better PSNR value which means we have recovered good quality of image and the lowest MSE rate which indicate the lower error rates of the reconstructed image.

6.1.3 Resampling

Resampling of the recovered doesn't gives us the proper original image due to huge loss in the bits of the image in three of the images. It has the lowest PSNR values which means the recovered image in this attack doesn't have good quality of image. The bit error rate of all the images is high which indicates huge drop in the bits of the recovered images.

7. Conclusion and Future Work

The main aim of this research was to overcome the vulnerability of the image steganography. We have successfully implemented this prototype which uses python script of 256-bit AES encryption for encryption and decryption of the secret message and we have used MATLAB for encoding the ciphertext in the image and stegoimage in the cover audio file. While extracting the image we have noticed that there is some loss of the bits. Because of loss in the bits, further it was difficult to recover the ciphertext from the stegoimage.

In future, we can try to use any other encoding algorithm for inserting the secret message in the image or audio file. This paper can be further extended to implement the better security using image steganography with any other strong cryptography algorithm and Video steganography.

8. References

- [1] R. Indrayani, H. A. Nugroho and R. Hidayat, "An evaluation of MP3 steganography based on modified LSB method," in *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*, Bandung, Indonesia , 2017.
- [2] K. Thangadurai and G. Sudha Devi , "An analysis of LSB based image steganography techniques," in *2014 International Conference on Computer Communication and Informatics*, Coimbatore, India , 2014.
- [3] S. Khan, N. Agmad, M. Ismail, N. Minallah and T. Khan, "A secure true edge based 4 least significant bits steganography," in *2015 International Conference on Emerging Technologies (ICET)*, Peshawar, Pakistan , 2015.
- [4] C. Arun and S. Murugan, "Design of image steganography using LSB XOR substitution method," in *2017 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, India , 2018.
- [5] V. V. Korgaonkar and M. N. Gaonkar, " A DWT-DCT combined approach for video steganography," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India , 2018.
- [6] S. K. Yadav and M. Dixit, "An improved image steganography based on 2-DWT-FFT-SVD on YCBCR color space," in *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, Tirunelveli, India , 2018.
- [7] S. Kamila and S. Changder, " A DWT based steganography scheme with image block partitioning," in *2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, India , 2015.
- [8] V. Kumar and D. Kumar, " Performance evaluation of DWT based image steganography," in *2010 IEEE 2nd International Advance Computing Conference (IACC)*, Patiala, India , 2010.

- [9] S. Jangid and S. Sharma, "High PSNR based video steganography by MLC(multi-level clustering) algorithm," in *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India , 2018.
- [10] S. MSP, "Understanding AES 256 Encryption," 29 07 2019. [Online]. Available: <https://www.solarwindmsp.com/blog/aes-256-encryption-algorithm>. [Accessed 28 10 2019].
- [11] B. Chernev, "What Is AES and Why You Already Love It," 12 03 2019. [Online]. Available: <https://techjury.net/what-is-aes/#gref>. [Accessed 30 10 2019].
- [12] Z. Wu, "Information Hiding in Speech Signal for Secure Communication," 12 09 2014. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B978012801328100001X>. [Accessed 20 10 2019].
- [13] D. B. Percival and D. Mondal, "22 - A Wavelet Variance Primer," 22 05 2012. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B9780444538581000223>. [Accessed 24 10 2019].
- [14] Y. Garg and A. kaur, " A Case study on Steganography and its Attacks," *International Journal of Engineering Trends and Technology(IJETT)* , vol. 47, p. 5, 2017.