A Study on Image, Audio and Video steganography

MSc Research Project
Cyber security

Bansie Vasudevan Iyengar
Student ID: X21121591

School of Computing
National College of Ireland

Supervisor: Mr. Jawad Salahuddin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Bansie Vasudevan Iyengar

Student ID: X21121591

Programme: Cyber Security **Year:** 2022

Module: MSc Research project

Lecturer: Mr. Jawad salahuddin

Submission Due Date: 15/12/2022

Project Title: A study on Image, Audio, and Video Steganography

Word Count: 3193 **Page Count: 15**

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.

Signature: Bansie Vasudevan Iyengar

Date: 11/12/22

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
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.	□

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):	

National College of Ireland

Contents

A STUDY ON IMAGE, AUDIO, AND VIDEO STEGANOGRAPHY

Abstract

Steganography is a practice of concealing or hiding secret information within a non secret multimedia to avoid detection. It can also be described as hiding information in plain sight. The word steganography comes from greek words “steganos” which means to hide or to be hidden and “graph” which means to write or embed. Steganography mainly deals with hiding sensitive information into multimedia to avoid detection, but this can be used alongside with encryption to make it even more secure during transmission of the multimedia. This paper presents a web application that enables the user to perform steganography on image, audio and video along with a strong encryption for the secret text message that is going to be embedded in the multimedia. This research is carried out so that the said web application can be developed and lets the user share sensitive information without worrying about the information getting stolen by an attacker and also this research can be improved further as every module is encapsulated and implemented as importable libraries.

Index Terms: steganography, cryptography, web application, fernet, LSB, DCT, echo hiding

Video presentation Link: https://www.youtube.com/watch?v=_e8FtxJu-tI

1. Introduction:

1.1. Background and overview:

Once people are used to the internet, it has emerged to be the most useful and efficient way of communication. Usage of the internet is growing so popular and quickly that it out ran satellite media within a decade. Most common people use the internet particularly messaging apps like WhatsApp, Facebook, Instagram to share and receive text messages, audio and video files. Apart from this there is also a lot of sensitive information that is transferred through the internet. There are various private sectors, medical fields or military organizations that send important information through the internet. As cybercrime is growing at an alarming rate, this could be very dangerous. A malicious attacker can easily use an open source tool to capture the entire traffic of the network and get a hold on the sensitive information that is being transferred in the network. To help with this situation, we are making use of a lot of cryptographic algorithms to make sure that the sensitive data is encrypted securely and only the intended receiver can decrypt it and view the information. One of the advantages of encrypting the text is that it is secure compared to plain text and only the person with the key can decrypt and read it. But one of the major disadvantages is that the attacker sniffing the network will also know that this is something important as it is encrypted and use the necessary tools to decrypt it. So, to overcome this, we combine the process of steganography and cryptography to encrypt the plain text and also hide the encrypted text in plain sight respectively.

1.2 Research question:

1)What is a steganography and what are its types? And why is it important?

2)what are the better generic algorithms and how modifications of those generic algorithm can make the encryption stronger and faster?

1.3 Motivation and value:

There are different types of steganography available:

1) Text steganography: This is a type of steganography in which a text can be encoded within each letter of another text inside a text file.

2) Image steganography: In this type of steganography, we use an image as the cover object and hide text inside an image. The more resolution the picture has the more data we can store in it.

3) Audio steganography: Audio steganography is in use for a long time now which protects the audio against unauthorized replication. It is also called audio watermarking.

4) Video steganography: This is a type of steganography where a video is used as a cover media to secretly embed text into it. As video is a collection of still images, discrete cosine transform is the most commonly used to hide data in every image of the video.

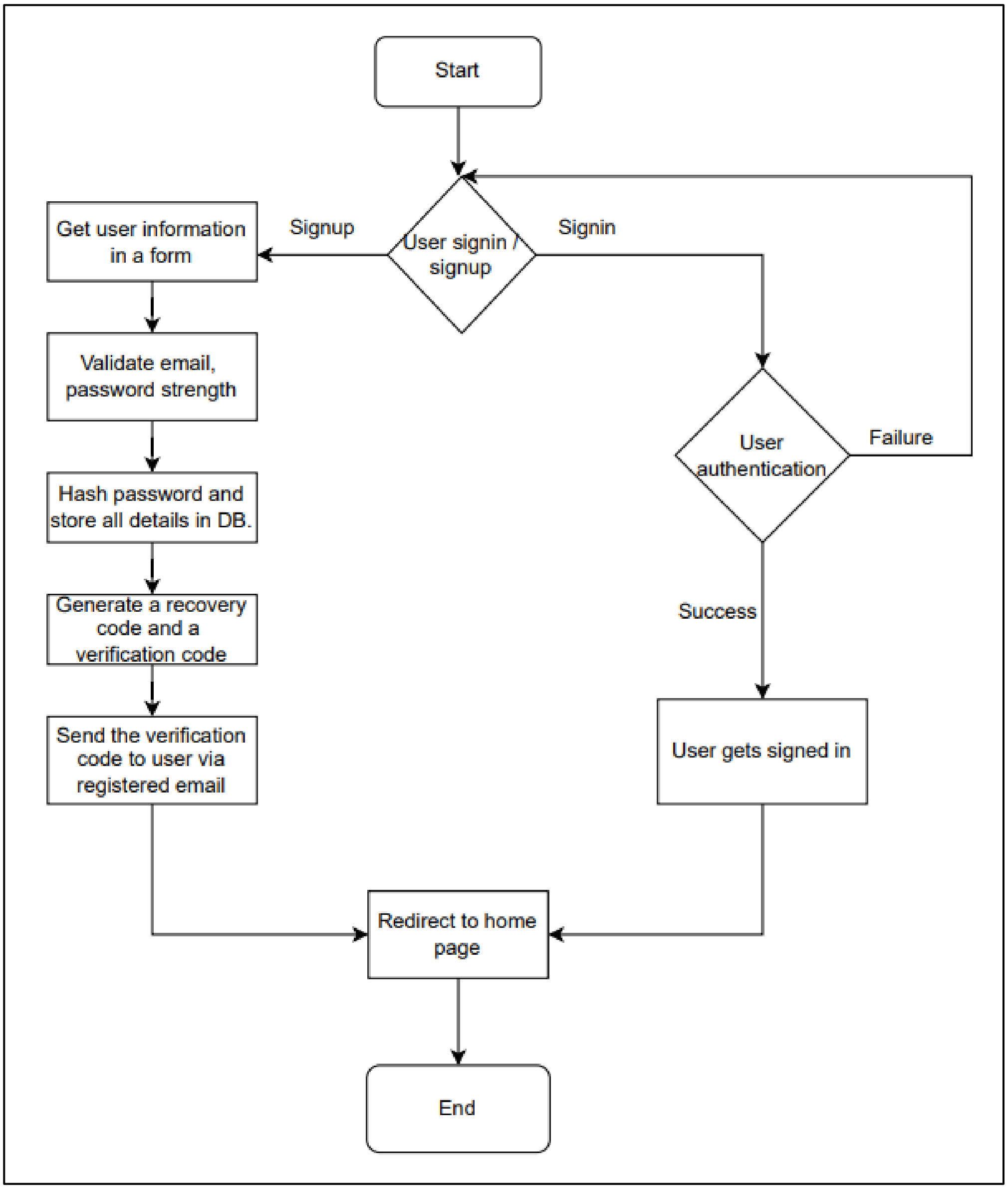
5) Network steganography: This involves in concealing data in a network protocol like TCP, UDP etc.,

The method that is proposed in this paper makes use of both the advantages of steganography and cryptography for added security and makes it easier for the user to use and navigate through by means of a web application. We are making use of techniques to make sure that the user's data follows the rules of CIA triad which stands for confidentiality, integrity and availability. The question for confidentiality is, 'who has the access to my data', the question for integrity is, 'who can modify the said data' and finally the question for availability is, 'do I have access to my own data' . The combination of steganography and cryptography provides the solution for the above questions and makes it complex and hard for the attacker to interpret the secret data.

1.4 Working of the web application:

In this research we will be focusing on the top 3 most used steganographic types which are image, audio, and video steganography.

First off, the user, both the sender and receiver have to create an account in order to use the web application, and once the account creation is done, they have to verify their account with the verification code that will be sent to their email id within 2 days. Once this is done the user is redirected to the home page of the web application where they can perform any kind of steganography they require.


Start
User signin / signup
Signup
Signin
Get user information in a form
Validate email, password strength
Hash password and store all details in DB.
Generate a recovery code and a verification code
Send the verification code to user via registered email
User authentication
Failure
Success
User gets signed in
Redirect to home page
End

e

Fig. 1 initial web application flow

1.5 General steganography procedure:

Plaintext (P) + Encryption_key (K) = Cipher_text (C)

Cover_multimedia (M) + Cipher_text (C) = Steg_multimedia (S)

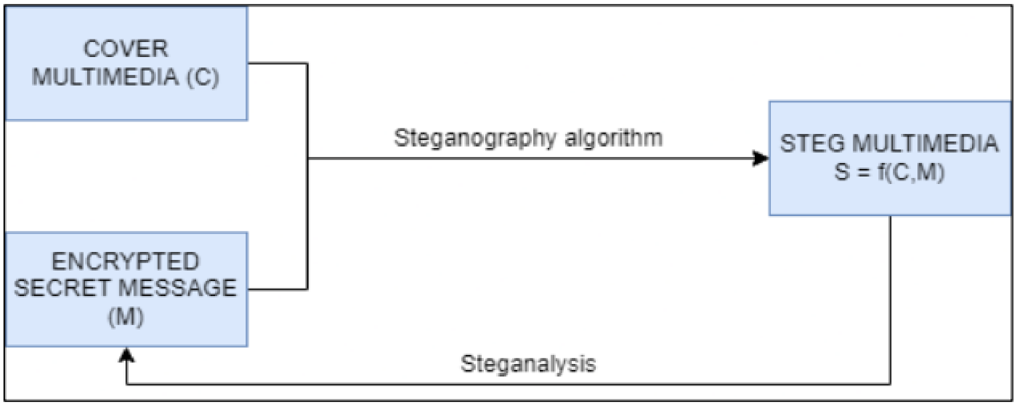


Fig. 2 steganography working

Once the user has completed the registration and logged in to the webpage, they are greeted with the different types of steganography that can be performed in the application. The sender can choose either image, audio, or video steganography. After choosing the appropriate type of steganography, the users will be redirected to the page to perform the steganography. If the users have chosen image steganography, then they will have to provide with the secret message, an image file and also the email id of the receiver. This is implemented in order to make sure that during decryption only the intended receiver is trying to decrypt the file. After the user has given all the necessary details, we can proceed with the actual steganography in the backend.

Firstly, the secret message provided by the user is encrypted using a 32 bit fernet key for 16 different rounds which comes up to 512 bit but with different key each round. Now this encrypted text is what being encoded in the multimedia using different algorithms in different steganography.

2. Literature Review:

2.1. Related work:

It is important to do a thorough literature review to comprehend the relevant research and the authors attempts to publish papers in the field of steganography and cryptography in order to fully grasp the uniqueness of the work. There have been various different techniques of steganography and cryptography in recent years which can be studied and enhanced.

2.2 steganographic techniques:

2.2.1 Traditional techniques:

LSB which stands for least significant bit is one of the most commonly used algorithms in image and video steganography. Images that has a very high resolution or pixel count is very much beneficial and effective for this method. The working of this algorithm is basically that, if some of the many pixels are altered, it should not distort or show any signs of tampering in the image or frame. The secret message will be converted into binary values and stored in the noisiest area of the image after scanning. However, this seems like a simple process, the scanning and embedding should be done with utmost caution because improper technique can result in distortion of the image or abnormal artifacts in the image which might compromise the secret message or raise suspicion.[1]

There exist various methods using the LSB approach. One of the most commonly used technique to convert secret plain text to binary is called Huffman coding. The resultant from Huffman coding can then be embedded into the image using LSB approach.[1]

Another type of LSB encoding uses the pixels in the image itself instead of scanning the noise in the image. This type makes use of the RGB values in the image. The cover image is split into 3 different planed that represent the red, green, and blue colour scheme. After splitting the text is embedded within the colours of the image so that the final result does not show any signs of tampering or image manipulation in it. This method is even more effective than the previous one because some images might have minimal to no noise after heavy processing, but those images will still have RGB planes and pixels.[1]

The same LSB technique can also be used to hide text in videos, as, videos are essentially multiple frames put together. A minimum of 24 frames combined together in one second forms a video. As we have a lot of frames, we can store a longer information inside video using this method [1][3].

2.2.2 CNN based steganographic techniques:

Most of the CNN based architecture works on the basis of encoder – decoder principle. Neural networks can be trained to analyse the input cover media and predict the perfect place that has a balanced amount of noise or making use of the already present image distortion to the advantage of steganography. Different types of convolutional layers, pooling layers, activation layers, and hyper parameters can be used that varies with each method [1][4][5].

2.2.3 Low bit encoding with audio:

There are other methods for audio encoding, but this is the quickest and easiest one. This works by encoding a little amount of data into the audio's least significant bit. A little amount of noise will be introduced after all the bits have been included into the audio. The method of steganography is successful if the induced noise falls below the threshold of audibility [6].

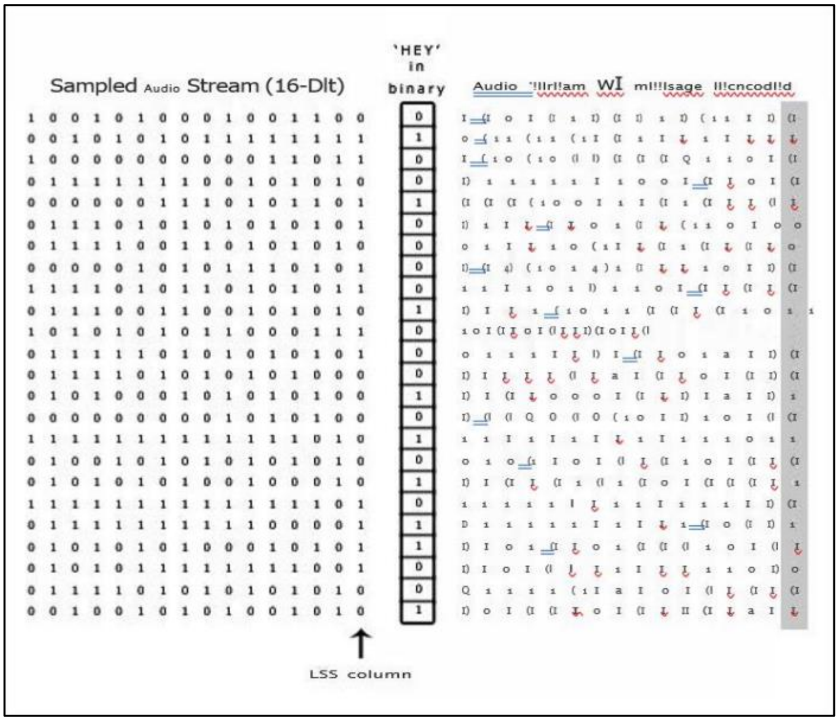

'HEY' in binary
Sampled Audio Stream (16-Dlt)
Audio '!Ilrl!am WI ml!!Isage Il!cncodl!d
LSS column

Fig. 3 Low bit encoding

Fig. 3 clearly explains the working of Low bit encoding on the word 'hey'.

2.2.4 Echo hiding with audio:

This type of encoding is very popular in audio watermarking research. There are several echo mechanisms such as single, bipolar, time spread, backward forward etc. This method mainly uses 3 different parameters to hide the data into the multimedia which are: decay rate, offset, and amplitude. These parameters are manipulated carefully to keep all the additional values under the human audible range [7].

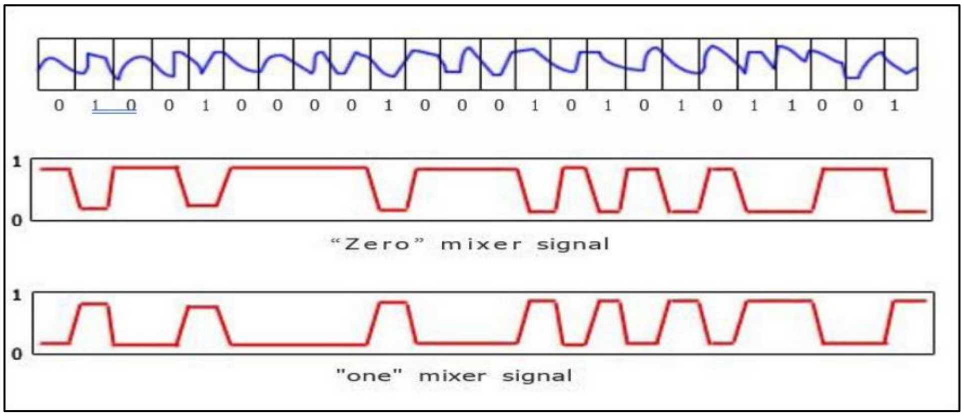
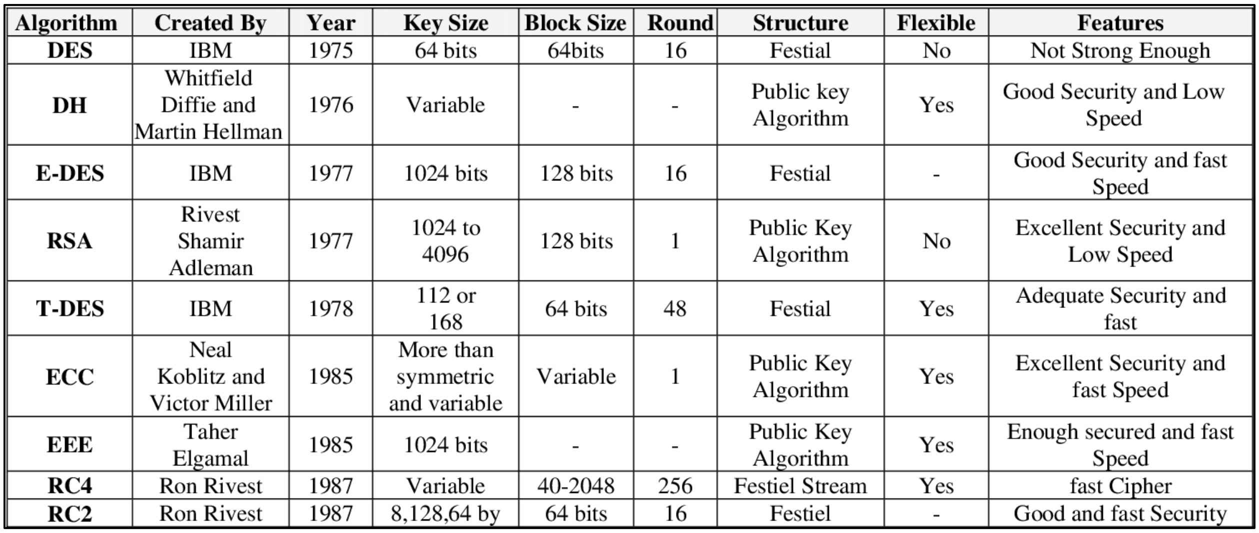


Fig. 4 Echo hiding

Fig. 4 shows the working of echo hiding in real time with zero and one mixer signals.

2.3 Cryptographic techniques:

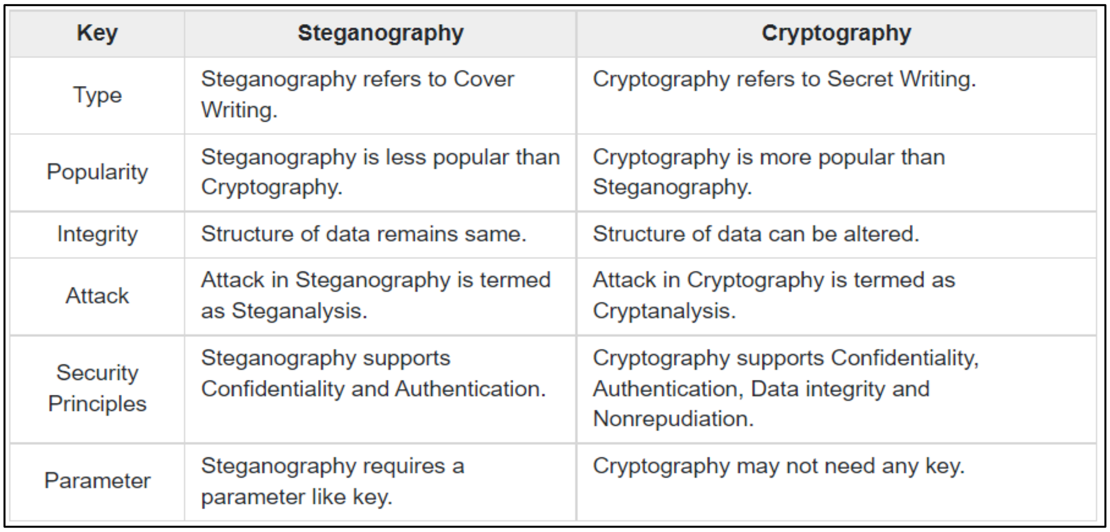
Some form of cryptography has been around since a long time before it was actually studied and implemented. Cryptography is basically defined as the process or technique of protecting sensitive data, so that it becomes hard to read and understand for the person to whom the data was not intended to. The main purpose of cryptography is not only protecting the data but also making sure the data's confidentiality, integrity, authentication, and non repudiation [4].



Algorithm	Created By	Year	Key Size	Block Size	Round	Structure	Flexible	Features
DES	IBM	1975	64 bits	64bits	16	Festial	No	Not Strong Enough
DH	Whitfield Diffie and Martin Hellman	1976	Variable	-	-	Public key Algorithm	Yes	Good Security and Low Speed
E-DES	IBM	1977	1024 bits	128 bits	16	Festial	-	Good Security and fast Speed
RSA	Rivest Shamir Adleman	1977	1024 to 4096	128 bits	1	Public Key Algorithm	No	Excellent Security and Low Speed
T-DES	IBM	1978	112 or 168	64 bits	48	Festial	Yes	Adequate Security and fast
ECC	Neal Koblitz and Victor Miller	1985	More than symmetric and variable	Variable	1	Public Key Algorithm	Yes	Excellent Security and fast Speed
EEE	Taher Elgamal	1985	1024 bits	-	-	Public Key Algorithm	Yes	Enough secured and fast Speed
RC4	Ron Rivest	1987	Variable	40-2048	256	Festiel Stream	Yes	fast Cipher
RC2	Ron Rivest	1987	8,128,64 by	64 bits	16	Festiel	-	Good and fast Security

Fig. 5 comparison of cryptographic algorithms (Abood, O.G. and Guirguis) [8].

3.0 Comparison of Cryptography vs Steganography:



Key	Steganography	Cryptography
Type	Steganography refers to Cover Writing.	Cryptography refers to Secret Writing.
Popularity	Steganography is less popular than Cryptography.	Cryptography is more popular than Steganography.
Integrity	Structure of data remains same.	Structure of data can be altered.
Attack	Attack in Steganography is termed as Steganalysis.	Attack in Cryptography is termed as Cryptanalysis.
Security Principles	Steganography supports Confidentiality and Authentication.	Cryptography supports Confidentiality, Authentication, Data integrity and Nonrepudiation.
Parameter	Steganography requires a parameter like key.	Cryptography may not need any key.

Fig. 6 comparison between steganography and cryptography

Fig. 6 compares and contrasts the differences between steganography and cryptography clearly. But the most important difference between them is that the structure of the input data remains the same in case of steganography and that's not the case in cryptography. There is minimal to no mathematical calculations in steganography whereas cryptography completely depends upon mathematical calculations.

4.0 Design specification:

In the proposed system, we are making use of both cryptography and steganography combining both the advantages and make the final resultant more safe and secure. To make sure that the encoding is safe from steganalysis attacks we have made use of 512-bit fernet encryption algorithm, which also prevents the attacker from brute forcing the encrypted text.

4.0.1 Image encoding / decoding process:

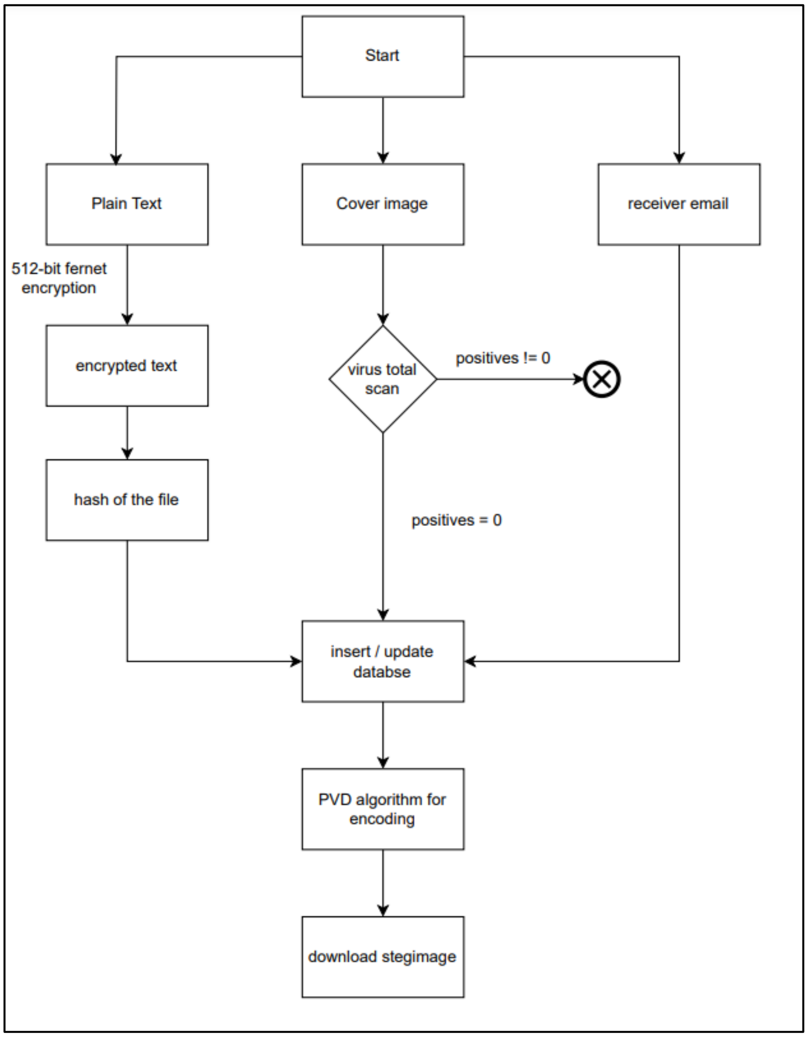


Fig. 7 image steganography encoding flow

Fig. 7 explains the prototype of the image encoding concept that has been implemented. The 3 main inputs that are gathered from the user is the secret message (secret plain text), the cover multimedia and the registered email id of the receiver. The plain text is encrypted using a 512 bit fernet encryption on 16 rounds with a 32-bit key each round. Parallelly the cover image is hashed and the hash is sent to virus total using an API for scanning. If the scan returns 0 positives, then we continue with the actual steganography process. The image is manipulated using the OpenCV library and we get the RGB values from the image. A secret delimiter is concatenated at the end of the encrypted text which can be used to identify the end of the text during decryption. Once the process is complete, the user is allowed to download the steg image.

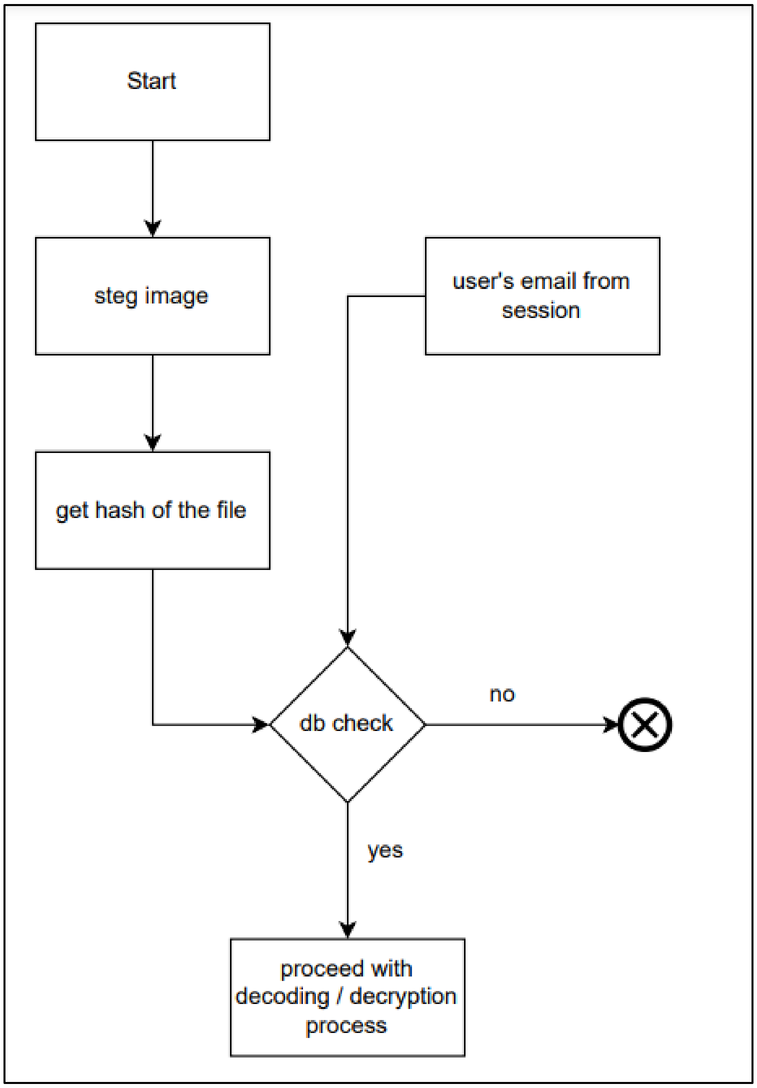

Start
steg image
user's email from session
get hash of the file
db check
no
yes
proceed with decoding / decryption process

Fig. 8 image steganography decoding flow

Fig. 8 clearly explains the decode / decryption flow. We only get the image file from the user and get the user's email id from the session. Then we hash the uploaded file and check the database for the matching hash which would be inserted during the encoding process. Once we find the matching hash we check if this user's email is present in the receiving email list, if it is present, we proceed with the decoding process. If it is not present, we are giving the user an error message and breaking the flow of the process.

4.0.2 Audio / Video encoding / decoding process:

The actual encoding and decoding flow for audio as well as video steganography is the exact same, the only thing differs is the algorithm that we use for encoding and decoding.

For Audio steganography, we are only allowing the user to upload and encode wav files because of 2 reasons:

- Wav is the most popularly used audio format around the world
- Wav is considered to have lossless compression when converted. So we will have a lot of bits so that when we encode the large encrypted text, it will not raise any suspicion.

We are making use of the WAV library that is available in python to manipulate the wav files. We are opening the audio files in binary mode so that we can read the frames from the file and convert it into bytearray so that we can embed the secret message to it. We strip all the empty spaces from the secret text so that it does not produce any noise in the actual audio file during encoding. we add a random delimiter that is calculated with the number of bits in the audio and the length of the secret text which will be used to find the end of the text when decoding the message.

In video steganography, we make use of both audio and image steganographic techniques that was previously discussed. As soon as the user uploads the video, the video is converted into frames and it gets stored in a temp folder, and we are making use of a 3rd party library called ffmpeg to extract the audio from the video. After this process we have a lot of frames and the audio extracted. So, we can perform image steganography on the frames and audio steganography on the extracted audio.

Once both the steganography is done in parallel, we can now collect all the frames and put it together to create the video again and add the audio to it along with a video and audio codec and the user can download the steg video.

5.0 Evaluation and case study:

The proposed system was evaluated in 2 main parts:

- The whole web application behaviour
- The steganography algorithm efficiency

The web application was tested different operating system and in different devices by changing the resolution in the web browser and it was found to be working without any issues. A list of test cases were created and checked multiple times in order to make sure that there are no corner cases in the application.

As far as the evaluation in algorithm in considered, Fig. 9 shows the difference between the original image and the stegimage after the encoding.

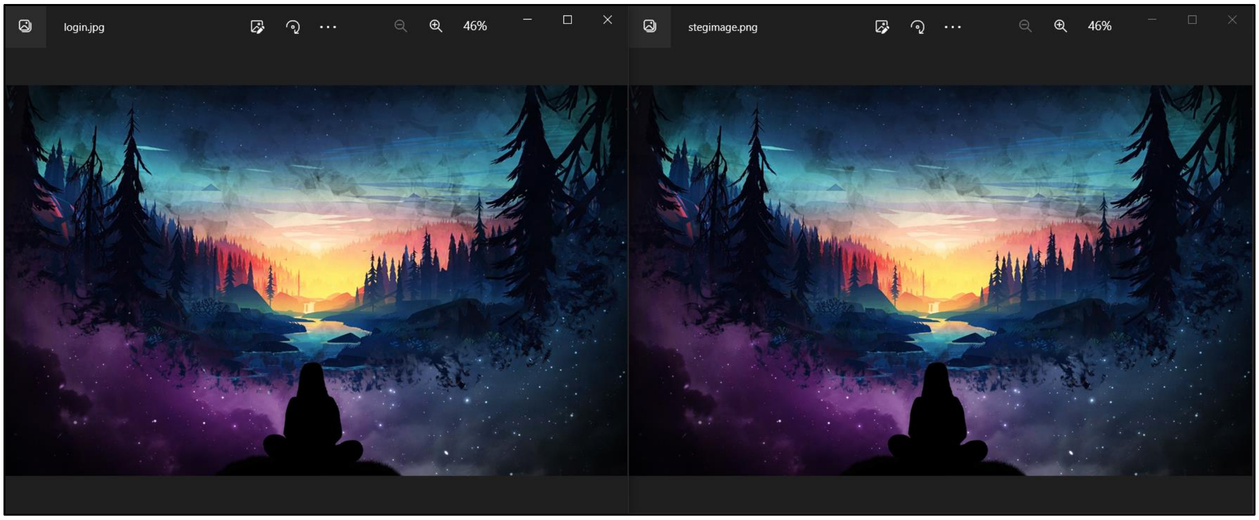
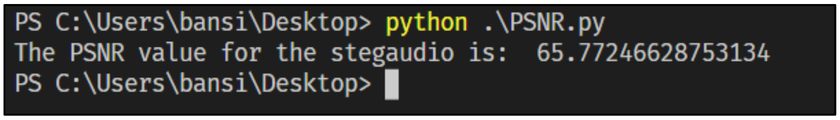


Fig. 9 image steganography evaluation

As we can see in the above image, both the images look the same. We don't see any forms of artefacts or distortion in the original image and the result.

For audio steganography, we calculated the PSNR value of the stegaudio with the original audio to make sure that the encoding algorithm is efficient and there are no distortions in the audio.



```
PS C:\Users\bansi\Desktop> python .\PSNR.py
The PSNR value for the stegaudio is:  65.77246628753134
PS C:\Users\bansi\Desktop> 
```

Fig. 10 PSNR value

Fig. 10 shows us the PSNR value of the stegaudio compared to the original audio and the PSNR value is found to be over 65% which is considered ideal when the embedded text is encrypted with a 512-bit key.

6.0 Conclusion and future work:

The implementation of Image, Audio, Video steganography along with encryption has been successfully executed. The goal of this research was to create a web application that enabled the users to perform steganography and transmit sensitive information in a safe and secure manner. Fernet algorithm with a 512-bit key was used to encrypt the plain text. There were security features implemented on the whole application right from sign up till session flushing.

6.1 Future work:

- Host the application in AWS cloud platform.
- User management and IAM roles should be managed by using AWS Cognito.
- User email services should be handled by Route 53.
- Using multiple encryption algorithms in random to make combinations higher so that it becomes impossible to brute force.

7.0 References:

[1] Ieeexplore.ieee.org. 2022. Image Steganography: A Review of the Recent Advances. [online] Available at: (Accessed: December 9, 2022).

[2] https://www.researchgate.net/. 2022. Comparative study of image steganography techniques. [online] Available at: (Accessed: December 9, 2022).

[3] Ach. Khozaimi, Sigit Susanto and Ainul Yaqin (no date) *Improve The Performance and Security of Medical Records using Fingerprint and Advance Encryption Standart , SCITEPRESS*. Available at: https://www.scitepress.org/Papers/2020/ (Accessed: December 9, 2022).

[4] NagaSrinivasuPersonEnvelope, L. *et al.* (2022) *CNN based "text in image" steganography using Slice Encryption Algorithm and LWT, Optik*. Urban & Fischer. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0030402622007173 (Accessed: December 9, 2022).

[5] W. Tang, B. Li, S. Tan, M. Barni and J. Huang, "CNN-Based Adversarial Embedding for Image Steganography," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 8, pp. 2074-2087, Aug. 2019, doi: 10.1109/TIFS.2019.2891237.

[6] M. Asad, J. Gilani and A. Khalid, "An enhanced least significant bit modification technique for audio steganography," International Conference on Computer Networks and Information Technology, 2011, pp. 143-147, doi: 10.1109/ICCNIT.2011.6020921.

[7] Kadir Tekeli and Rıfat Aşlıyan (no date) *(PDF) a comparison of Echo hiding methods - researchgate*, *A COMPARISON OF ECHO HIDING METHODS*. Available at: https://www.researchgate.net/publication/326720071_A_COMPARISON_OF_ECHO_HIDING_METHODS (Accessed: December 9, 2022).

[8] Abood, O.G. and Guirguis, S. (1970) *[PDF] a survey on cryptography algorithms: Semantic scholar, undefined*. Available at: https://www.semanticscholar.org/paper/A-Survey-on-Cryptography-Algorithms-Abood-Guirguis/21b1d62956dba6b71b363e588a2aa4bbb117fcaa (Accessed: December 10, 2022).

[9] Wave - read and write WAV files (no date) *Python documentation*. Available at: https://docs.python.org/3/library/wave.html (Accessed: December 10, 2022).

[10] GyanD (no date) *Release ffmpeg git 2022-06-06 builds · gyand/codexffmpeg, GitHub*. Available at: https://github.com/GyanD/codexffmpeg/releases/tag/2022-06-06-git-73302aa193 (Accessed: December 11, 2022).