National College of Ireland

Using AES Encryption to Securely Embed Data in Video Files

MSc Research Project

M.Sc. in Cybersecurity

Dhruvesh Parekh

Student ID: 20182457

School of Computing

National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Dhruvesh Chetan Parekh……

Student ID: x20182457……..……

Programme: MS in Cybersecurity…… **Year** 2021-2022

Module: Research Project……..……

Supervisor: Vikas Sahni……..……

Submission Due Date: 26/04/2022……..……

Project Title: Using AES Encryption to Securely Embed Data in Video Files.

Word Count: 5123 **Page Count:** 23

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: ……Dhruvesh Parekh……

Date: 25/04/2022……

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):	

Using AES Encryption to Securely Embed Data in Video Files.

Dhruvesh Parekh

X20182457

Abstract

Data piracy, illegal access, and data loss have all become major concerns in recent years when it comes to safe data exchange. Hackers can easily intercept and manipulate data if it is not transmitted correctly. As a result, data security has become a key research topic. The use of cryptography and steganography together has been shown to be advantageous. Cryptography is the science of encrypting data, whereas steganography is the art of hiding text inside any multimedia file. The goal of this work is to provide a novel method for hiding information in a video, by combining cryptography and steganography. To protect against any cyber-attack, the message is first encrypted using the AES technique, where the key is hashed using SHA-2, followed by a modification of the LSB method by including a key to make the hiding process non-sequential, in terms of robustness and security.

Keywords – Data Transmission, encryption, decryption, Advanced Encryption Standard, Cryptography, Steganography.

1 Introduction

The necessity for security grew as Computer services began to deal with personal and financial data. Data on personal computers is an essential component of front-line living. Security is now necessary to securely transfer data from one place to another. An intruder is on the opposite side of impenetrable security. Because it is concerned with security, cryptography is one of the most significant concepts in today's secure communication environment. Cryptography is the process of encrypting messages such that they become unintelligible. If an attacker finds that the data is safe, he or she may try to decode it with a specific set of keys.

One reason intruders may be so effective is that the majority of the information they steal or obtain from a system is in a format that they can read, alter, and change. Intruders may spread the data, alter it to represent a person or group, or use it to launch an attack. Steganography is one answer to this problem.

2 Related Work

Electronic communication (EC) is vital to many businesses. Every piece of data sent on a daily basis must be kept private. Confidential reports, records, and worker information should be delivered in a secure and confidential manner. This is a sound financial decision that may even be regulated by legislation, comparable to the HIPAA (Health Protection, Transportability, and Responsibility Act) (Yee, 2017). Most of this data is carried through the open web and may be handled by other parties, such as e-mail creating the problem of instant messaging (IM) (Ezhilarasi, 2019).

As previously said, the amount of data shared via the Internet increases the importance of network security. This problem inspires instructors to conduct a number of research in order to increase their ability to deal with security issues. Integrating the benefits of cryptography and steganography into a single system is one answer to this challenge. Many studies have proposed strategies for combining cryptography and steganography into a single system. These methods have previously been found to be extinct in previous surveys on the subject.

A survey by Feng & Buyya, 2016 was published in 2016 that aimed to give a broad overview of the proposed strategy of merging cryptography and steganography technologies. The authors detailed and compared 12 techniques that integrate steganography and cryptography... Security factors such as authentication, confidentiality, and resilience were used to make this comparison. Another review (Wagh, et al., 2020) was published in 2020, and it covered the Alteration Component, AES Algorithm, Distortion Process, Random Key Generation, and Key Based Security Algorithm, among other steganographic methodologies combined with cryptography.

In a study by AL-Shaaby, 2020 several encryptions and steganography techniques were utilised to hide data in a video. These tactics varied based on the resources available and the module being used by the users. The methods used were the Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and the Pixel Value Differencing Method. Based on the soundness of the provided algorithm, the authors concluded the study by proposing AES as the most widely used video-concealing approach.

The study (N. Patel, 2016) examined numerous symmetric encryption algorithms, including 3-DES, RC5, Blowfish, and AES, and found that AES offers the best combination of block sizes, rounds, flexibility, and security. The Hex-Symbol algorithm has been demonstrated to be more efficient than previous symmetric algorithms; therefore, traditional steganography approaches are also compared to it.

The cover video frame was used in the study (K.S. Seethalakshmi, 2016), and secret data was introduced using a lookup table and a 2bit LSB method in non-completed form. The look-up table showed how many times the secret data bits had to find perfect matches with the cover frame's pixel bits. The optimal match approach increased the calculation time, which was a

downside of the proposed strategy. To overcome this problem, a non-complementary method was offered. In terms of accuracy, this technique surpassed previous alternatives.

The author, Mohammad Shirali Shahreza (M. S. Shahreza, 2005) used LSB pixel colors to develop steganography for mobile phones. Each bit of data is buried in two pixels, with the three colors dividing the data into eight bits (RGB). Due to the low sensitivity of the human eye, the LSB method improvement may go unnoticed. They used a lossless PNG image with a little file size. If the data is modest in contrast to the size of the image, the bad actor can use traditional steganography methods to recognize the pattern of shifting pixels and extract the secret information.

Technology progress has a tremendous influence on human lives. As technology makes people' lives simpler, it needs increased security. Steganography is a technique for hiding personal and sensitive information in images, allowing for safe and untraceable communication between several people. Even under the strictest conditions of continuous observation, steganography allows data to be delivered secretly through any digital communication medium. It is possible to communicate and exchange data in secret without being caught, and no one can predict the presence of a secret message disguised within a photograph (S. Bukhari, 2016). The embedding is achieved by reducing the properties of other content, such as photos, audio, and video files, which are frequently referred to as coverings.

The finished result retains the original cover media properties. The crucial information is concealed under cover. When secret data is behind a cover image, a stego picture is formed. The work by Singhal & Prakash, 2020 introduced the concept of steganography as well as various steganographic video approaches. The National Security Agency of the United States devised SHA-256, which was eventually adopted and published in 2001. The digest is a SHA-256 cryptographic hash. It generated a one-of-a-kind 256-bit (32-byte) text code. A hash cannot be decrypted to disclose the original data because it is not an encryption mechanism. From the provided text, it created code of a predefined size. It's a cryptographic function that only works in one way. The hash version of the text was the only one that was compared, which boosted security. It avoids providing passwords in their original format; hence, even if the communication is intercepted through media or channels, the interceptor will never obtain the original password.

According to the NIST (National Institute of Standards and Technology), it has never been compromised (R. Das, 2016). AES is a cryptographic technology for encrypting textual data in an unreadable manner. It is also the safest encryption standard available, with no proof of breach. It is a symmetric key algorithm, which means it encrypts and decrypts with the same key. It uses 128-bit, 168-bit, 192-bit, 224-bit, and 256-bit block encryption. XOR, substitution, permutation, and row and column shifting are among the methods used by AES.

In (Almuhammadi, 2020), the authors described an image steganography approach. They used the DES algorithm to encrypt the text message at first. They used a 16-round DES with a 64-bit block size. After that, the pixels are clustered using KMeans Clustering, which separates

the image into many segments, each containing embedded data. A number of clustering approaches are used for image segmentation. The process of segmentation requires a huge quantity of data in the form of pixels, each of which contains three components: Red, Green, and Blue (RGB). After the clusters are built, the encrypted text is divided into K segments. In each cluster, these portions must be concealed. They employed the LSB approach to do this.

Table 1: Table of Approaches and Algorithms comparison from Study [10].

AUTHORS	APPROACHES/ ALGORITHMIC TECHNIQUES	OUTCOME
United States National Security Agency (NSA), 2001	Secure Hash Standard	Hash value is obtained containing 256-bit hash value.
Charles G. Boncelet, Jr, Newark, DE (US); Lisa M. Marvel, Churchville, MD (US); Charles T. Rettes, Belcamp, MD (US), 2003,	Spread spectrum and image steganography	It generates a spreading Sequence with a pseudorandom noise generator by a key, modulates the encoded text by the Spreading Sequence to obtain an embedded Signal and merging the embedded signal with a cover Signal to generate a StegoSignal
Po-Yueh Chen* and Hung-Ju Lin, 2006	A DWT based approach for image steganography	Data is embedded in the image with a secure key matrix.
Domenico Bloisi and Luca Jgcchi, 2007	Image based steganography and cryptography	A unified approach using ISC as in cryptography and steganography.
Ali AL-Ataby and Fawzi Al-Naima, 2010	A modified high-capacity image steganography technique based on wavelet transform	Data is hidden in the image with wavelet transformation in message as well as image.
Shailendex Gupta, Ankur Goyal, Bharat Bhushan, 2012	Information hiding using least significant bit steganography and cryptography	RSA and Diffie Hellman algorithm has been used as cryptography technique to generate cipher text and LSB is used to embed it into image.
Saiful Islam*, Mangat R Modi and Phalgvai Gupta, 2014	Edge-based image steganography	Hiding of data into the image edges is achieved.
Khan Muhammad, Jami Ahmad, Haleem Farman, Muhammad Zubair, 2015	A novel image steganographic approach for hiding text in color images using HSI color model	It contains larger Peak Signal to Noise Ratio (PSNR) valves.
Khan Muhammad, Jamil Ahmad, Muhammad Sajjad, Muhammad Zubair, 2015	Secure image steganography using cryptography and image transposition	Multiple encryption (bitxog operation, bits shuffling, and stego key-based encryption) and Image transposition is done for data hiding.
Mocatlag Abu-Abaiia, 2019	Crypto-Steganographic LSB-based System for AES-Encrypted Data	Stego image is obtained with cipher text by AES-128-bit encryption.

3 Research Methodology

This research paper embedded two technologies i.e., steganography and cryptography to hide the information. Firstly, the secret message is encrypted with the help of AES algorithm and to hash it's key SHA-2 algorithm is used. later on, that encrypted data is embedded into the source file i.e., video via LSB method. The sender and the receiver must have the same key to successfully decrypt and encrypt the data. So, to make the technology more secure and protect against attacks, this technology implements both cryptography and steganography instead of using them separately. This encrypted message can be embedded into any medium. The key for the AES algorithm and the key for the encryption method will be agreed upon by the sender

and receiver, or these keys will be communicated over a secure communication channel. This method starts with encrypting data and then concealing it.

Figure 1 represents the sender side of this approach, whereas Figure 2 represents the receiver side of this technique.

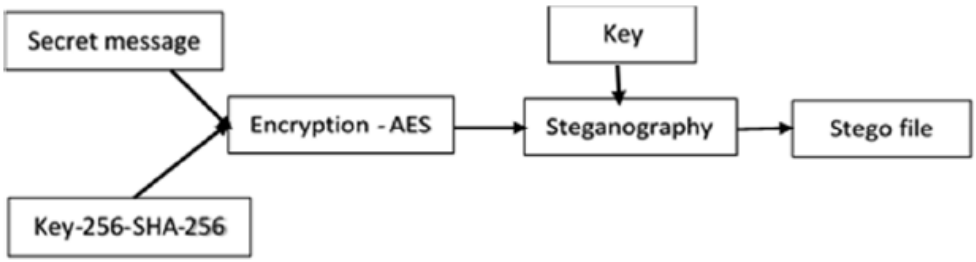

Figure 1: Sender.

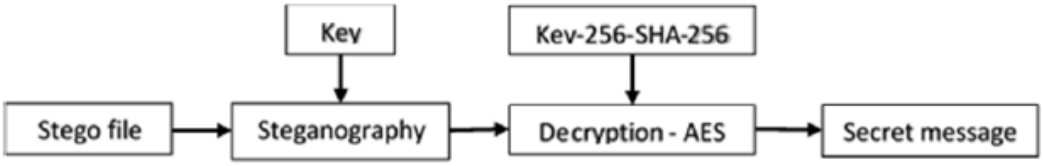

Figure 2: Receiver.

In table-1 these algorithms include AES, Blowfish, 3DES, and DES, as well as a variety of comparison criteria such as block size, key length, structure, and others. On the bases of these considerations, AES looks to be the most powerful symmetric key algorithm currently in use.

Table 2: Comparison of Symmetric key Algorithms [19]

Method	DES	3DES	AES	Blowfish
Developed by	IBM	IBM	NIST	Bruce Schneier
Structure	Feistel Network	Feistel Network	Substitution and Permutation Network	Feistel Network
Key Length	56 bits	Three 64 bits	128bits,192 bits, 256 bits	Variable length with max 448 bits
No. of rounds	16	48	9	16
Block size	64	64	128	64
Efficiency	Slow	Slow	Highly Efficient	Highly Efficient
Vulnerabilities	Brute Force Attack	Theoretical Attack	Side channel Attack	Not Prone to Attack

4 Design Specification

4.1 AES Algorithm: -

The researchers use the AES symmetric cryptosystem standard. AES is a block cipher that uses a 128-bit data block length. AES supports three alternative key lengths: 128 bits, 192 bits, and 256 bits. Any AES algorithm requires a varying number of processing rounds depending on the key length (Ezhilarasi, 2019).
Data block lengths i.e., 128-bit, 128-bit, 192-bit, or 256-bit keys are available. AES is an iterative algorithm in which "Round" refers to a single full iteration (Singhal & Prakash, 2020). The total number of rounds Nr is determined by the key length N_k. The 128-bit data is broken down into 16-byte chunks. These bytes are mapped to a 44-byte array called the state, which is used for all AES operations.

Each round consists of four steps:

- Byte substitution step
- Row wise permutation step
- Column wise mixing step
- Addition of Round key

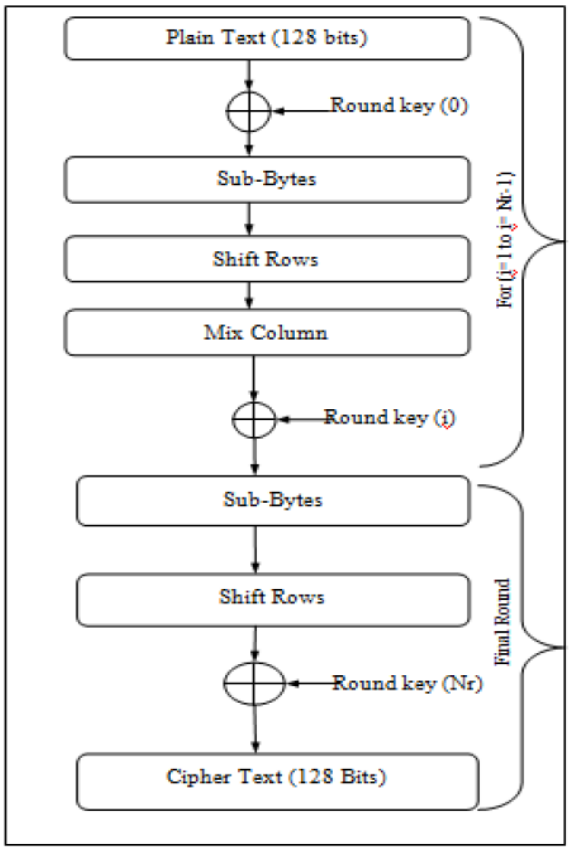

Figure 3. The AES encryption block diagram shows the several processes that are carried out based on Nr and Nk.

The key size variants and their accompanying rounds are as follows:

Key Length (Nk)	Block size (Nb)	No. of rounds (Nr)
4x32 = 128bits	4x32 = 128bits	10
6x32 = 192bits	4x32 = 128bits	12
8x32 = 256bits	4x32 = 128bits	14

Table 3: AES Parameters.

If the key length is less than the number of bits required for a particular AES method, the length should be raised using the zero-padding strategy. When the required key length is more than the number of data bits, like in AES-192 and AES-256, the key expansion technique is used to extend the key length.

4.2 LSB Algorithm: -

The most frequent approach for embedding message bits with DCT coefficients is LSB embedding (N. Patel, 2016). In the spatial domain, this method has been used to inject a zero or a one into a pixel's least significant bit value. Assigning an even coefficient to a zero-bit value and an odd coefficient to a one-bit value is a simple example. In order to embed a message bit in a pixel or a DCT coefficient, the sender raises or lowers the value of the coefficient/pixel to insert a zero or a one. The secret message bits are then retrieved by reading the same sequence of coefficients and decoding them using the encoding procedure.

The benefit of LSB embedding is that it has a high embedding capacity and that the change is typically unnoticeable to the bare eyes. When all of the coefficients are employed, the frequency domain approach can give a capacity of almost one bit per coefficient. On the other hand, with nearly 1 bit per pixel for each colour component, it can give more capacity for spatial domain embedding. Sending a raw picture, such as a Bitmap (BMP), to the recipient, on the other hand, might raise suspicion unless the image file is very tiny. Fridrich et al. suggested a steganalysis approach for detecting shorter concealed messages with a high detection rate.

For BMP pictures, Westfeld and Pfitzmann (Parik & Amin, 2016) suggested a new steganalysis procedure in which the message length is similar to the pixel count. The majority of today's popular formats are compressed in the frequency domain, hence embedding bits directly in the spatial domain is uncommon. As a result, for picture steganography, frequency domain embeddings are the favoured method.

4.3 Cryptography vs Steganography: -

Table 4 compares steganography with cryptography based on a variety of parameters. The comparison is based on the following criteria: definition, objective, security services provided, attacks, type of attack, carrier, visibility, input file, key, result, applications. Comparison of Approaches and Algorithms by Ahmed AL-Shaaby [2].

Table 4: Cryptography vs Steganography

Criteria/Method	Steganography	Cryptography
Definition	Cover writing [7, 1]	Secret writing [7, 1]
Objective	Maintaining existence of a message secret ,Secret communication [7, 1, 5]	Maintaining contents of a message secret ,Data protection [7, 1, 5]
Carrier	Any digital media [7, 1, 6, 10, 8]	Usually text based [7, 1, 6, 10, 8]
Input file	At least two [6]	One [6]
Key	Optional [6, 7, 8, 1]	Necessary [6, 7, 8, 1]
Visibility	Never [6, 1, 7]	Always [6, 1, 7]
Security services offered	Authentication, Confidentiality, Identification [10]	Confidentiality, Identification, Data Integrity and authentication Non-repudiation [6, 7, 1, 10]
Type of Attack	Steganalysis: Analysis of a file with an aim of finding whether it is stego file or not [6, 1, 10, 8]	Cryptanalysis [6, 1, 10, 8]
Attacks	Broken when attacker reveals that steganography has been used. known as Steganaly-sis. [6, 5, 7, 1]	Broken when attacker can understand the secret message. known as Cryptanalysis [6, 5, 7, 1].
Result	Stego file [6, 1, 8]	Ciphertext [6, 1, 8]
Applications	Used for securing information against potential eavesdroppers [10]	Used for securing information against potential eavesdroppers [10]

5 Implementation

The suggested approach for data concealment is based on video steganography, with the AES algorithm being employed to improve the steganography's security and robustness. The video steganography is accomplished by embedding the secret data to be communicated within the video files, with the goal of maintaining the secret data unchanged or intact at the receiver's end.

5.1 Advanced Encryption Standard (AES)

The AES algorithm is the most secure and resistant to cyberattacks of any cryptographic method. DES, on the other hand, is extremely slow and has previously been broken, as it generates wasteful software code. Triple DES is slower than DES since it contains three additional rounds.

As AES is a symmetric block cipher, the encryption and decryption keys are the same. AES's block size ranges from 128, 192, and 256 bits, and it performs substitution and permutation. The number of rounds is determined by the key length, which is 10 for 128 bits, 12 for 192 bits, and 14 for 256 bits. The researcher also chose SHA-1 to provide a more limited methodology just because it creates the hash function with a key, which helps to keep the secret data private because it can never be altered if it is recognized without the key. The next step is to do true steganography, which involves hiding this secret data inside the video carrier and creating a stego video as a result of video steganography.

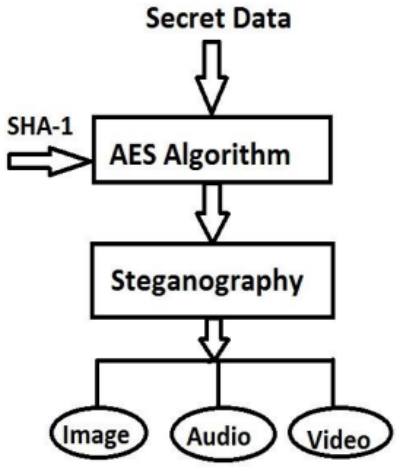

Figure 4: The Proposed Steganography.

5.2 Extraction of video file (at Sender Side)

The video steganography process is divided into two phases: video file extraction and secret message embedding. Because the secret message is already encrypted with AES and SHA-1, it can be readily integrated into carrier video. As video is often made of still images and sounds, the audio and image frames from the video file are extracted. The stego file is created from this extracted audio because the secret data is hidden in the audio rather than the picture frames. Secret data may be easily hidden in audio because it contains unused bits or free bits of information. The stego file is again encrypted using the Advanced Encryption Standard to make it more resistant to intrusion or identification. This is because of this extensive data hiding approach, the stego file created is subsequently transferred via the communication channel, which remains intact. The step of extraction is as follows.

On the sender's side, cryptography is the first step in this process, followed by steganography.

5.3 Encryption Stage:

The researchers have utilised the Advanced Encryption Standard (AES) approach with a 256-bit key and a 128-bit Block Size to encrypt the secret message. This approach encrypts data with a 14-character password (8 bits per character), which is then sent to the receiving end for decryption. To make it compatible with future processing, the encrypted message is converted from UTF-8 to base64. The data is subsequently written to a file and saved for further processing. To protect the key from attacks, we utilized SHA-2 hashing (SHA-256). This data which has been encrypted will be used in the steganography process.

Input= private key + secret message -------- (1)

Output= encrypted message --------- (2)

5.4 Steganography Stage:

Least significant bits (LSB) with fewer modifications have been used by author and other researcher in the stenography stage to hide the encrypted data into a file, whereas in this approach the author makes use of Videos to hide the data, instead of images and audio. In a non-sequential approach, the final bit in each frame is utilized to hide one of its binary stream bits. The last bit in each frame is used to conceal one of its binary stream bits, which is a generic LSB technique for concealing secret information. Each cover image's last bit is encrypted, which is a generic LSB strategy for hiding secret information in a file. However, in order to improve LSB, the author wants to make certain changes to our approach. As a consequence, researchers experimented with various mathematical methods based on the key provided by the user to perform the hiding operation at random rather than sequentially.

Methodology should be followed [15]:

Input= encrypted message + private key+ cover image ------- (3)

Output= stego-video ------- (4)

1. Take a look at the key and the secret message first.
2. All of the secret messages must be converted to binary.
3. Provide a special code at the end of the paragraph that may be used to get the concealed key.
4. Choose an acceptable video size for the concealing operation.
5. Read the character from the text and compute the ASCII formula in bytes, then divide the byte into three segments, the first of which includes (2) the first two parts and the second and third portions, each of which has (3) bits in the sequence.
6. read the first pixel of the picture.
7. Convert the pixel value to binary format.

   For example, the first pixel contains R = 200, G = 210, and B = 186 values. In addition, the key is =9.

Also, the secret message is (K), thus each color's binary value is as follows: Red = (1100 1000)
Green = (1101 0010)
Blue = (1011 1010)
And here's the hidden message: (0110 1011)

8. Hide two bits of the secret message in color R's LSB, three bits in color G's LSB, and three bits in color B's LSB. The values of the new color will be as follows:
G= (11010010) =210 B= (1011 1011) =187 R= (1100 1011) =203 G= (11010010) =210 B= (1011 1011) =187
9. To compute the hidden space, add four bits from any color to the key.
If we use G (0010) = 2 as an example,
S= (N)2 +(Key) ------- (5)
S=2+9=11 is the space.
10. Determine the next pixel in order to hide information within it. Using the axis, the researcher can now access pixels (X, Y).
As a result, the following pixel equals (X, Y+S) ------- (6)
If we are in pixel (5,34), for example, the following pixel will be (5,34+11) = (5,45).
Pixel is the next potion to be hidden in it (5,45).
11. Steps 5, 6, 7, 8, 9, and 10 should be repeated until the text's end code appears.

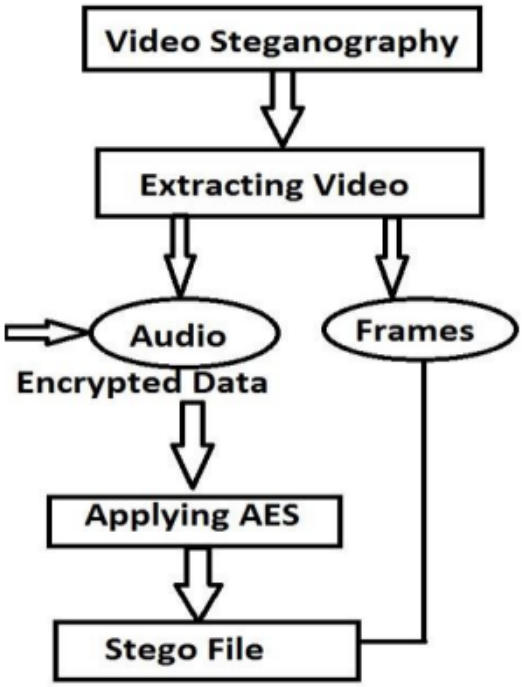

Figure 5: Extraction of Video at Sender side.

5.5 Extraction Of Stego File (at Receiver Side)

At the receiver's end, the stego file may be retrieved by first decrypting it and then extracting the carrier video, which is nothing more than a collection of audio and image frames. The resulting data is encrypted secret data, which must be decoded again to access the original data. Thus, the suggested method uses two layers of encryption, the first on the secret data itself and the second on the audio file, to give the most secure technique. The step of extraction is as follows.

On the receiver side, steganography and cryptography stages can be detected. They try to collect the embedded data first, then decode it on the receiver's side.

5.6 Steganography Stage:

The researchers start with steganography and then go on to cryptography on the receiving end. They shall proceed in the same manner as the sender.

Input= stego-video+ private key ------- (7)

Output= encrypted message ------- (8)

5.7 Cryptography Stage:

To decode the contents of the stego file, the researchers utilized the Advanced Encryption Standard (AES) technique with a key length of 256 bits and a block size of 128 bits. Researchers will proceed in the same manner as the sender.

Input= encrypted message + private key ------- (9)

Output= secret message ------- (10)

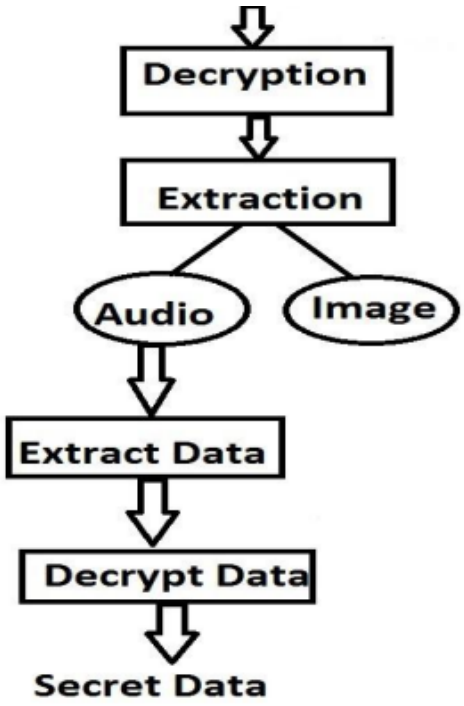

Figure 6: Extraction of Stego File at Receiver Side.

5.8 Flowchart:

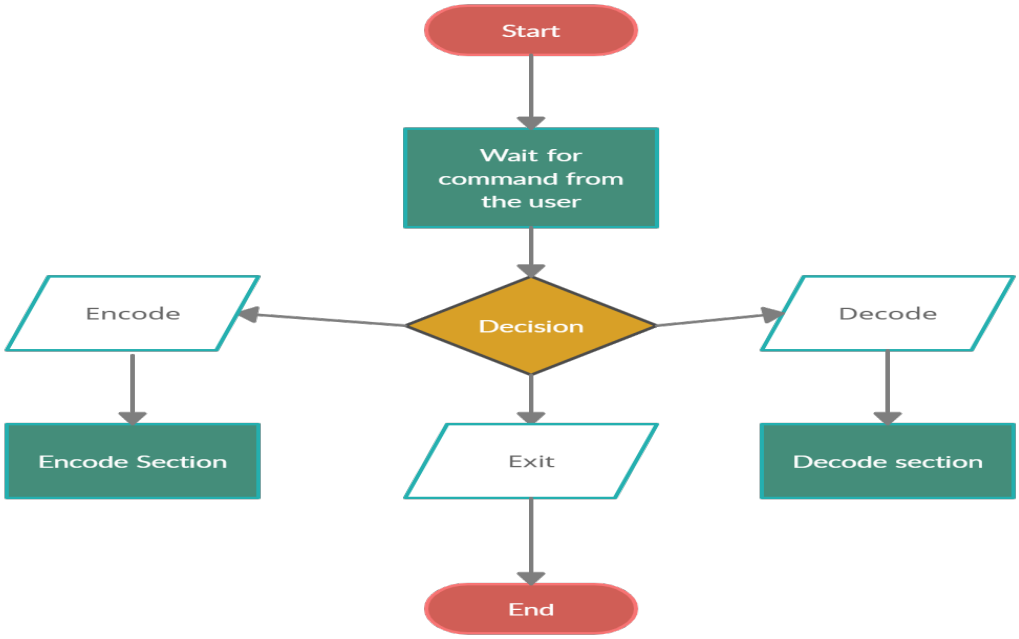

Figure 7: Main Interface Diagram

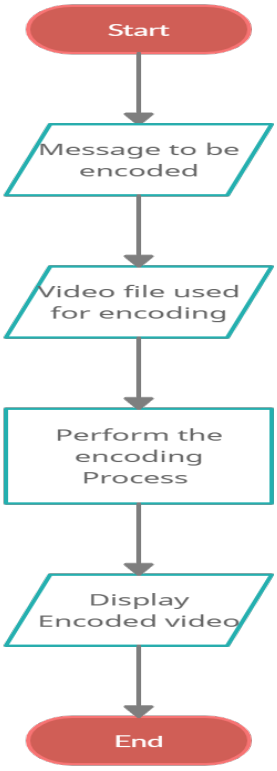

Figure 8: Encryption Diagram

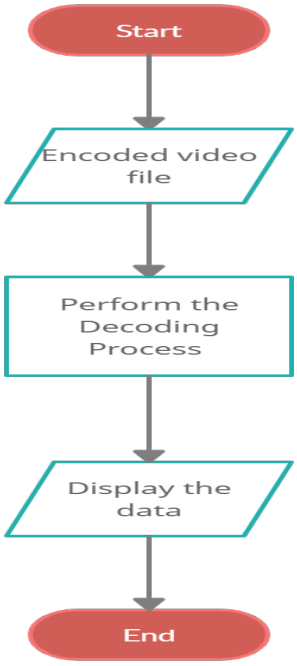

Figure 9: Decryption Diagram

5.9 Use Case:

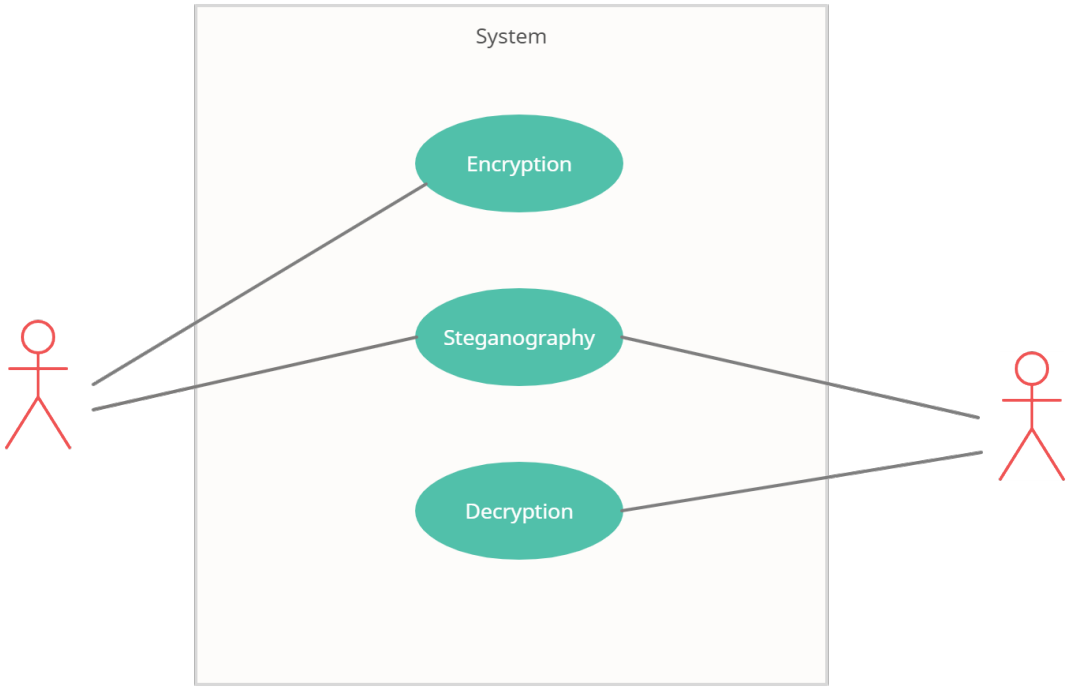

Figure 10: Use Case

5.10 Sequence Diagram:

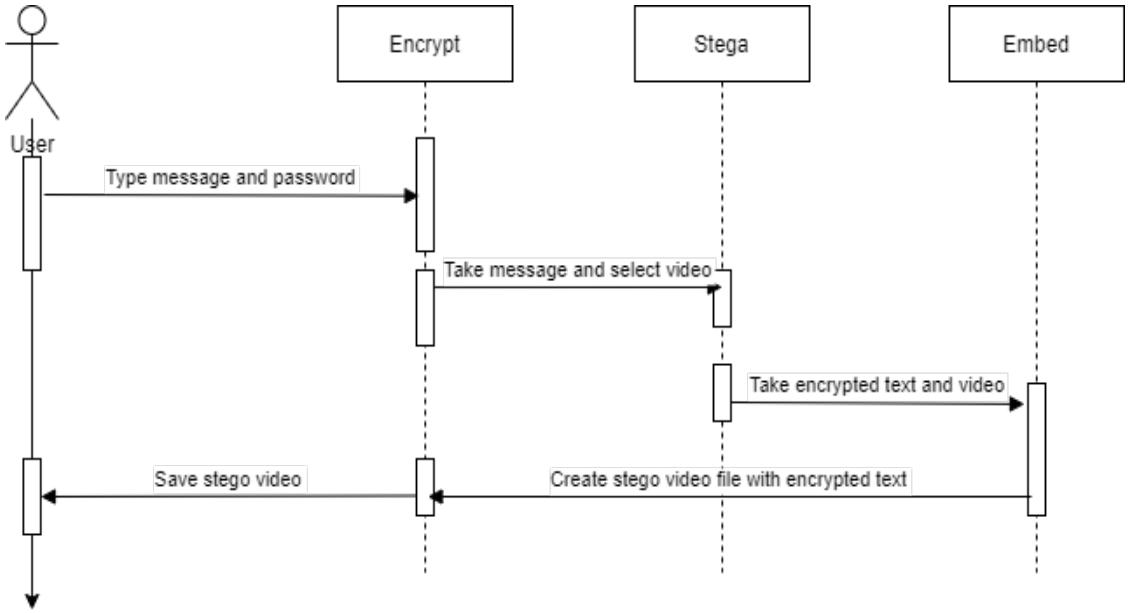

Figure 11: Encryption

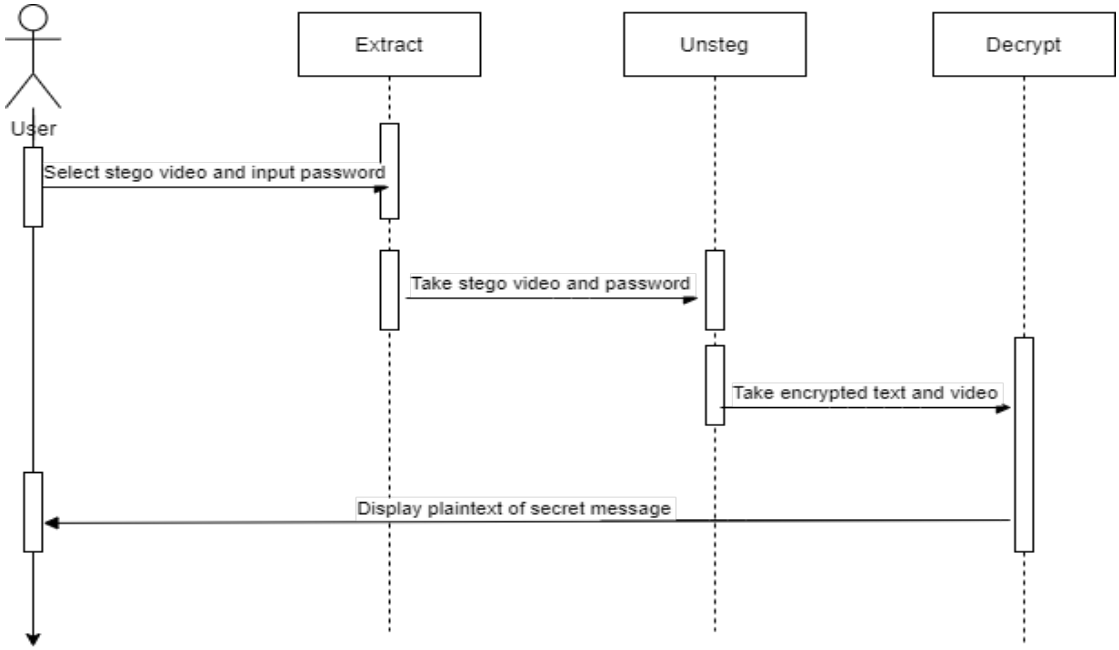

Figure 12: Decryption

6 Evaluation

The AES algorithm is used in video steganography to transport information from one end to the other. Several methodologies and metrics may be measured objectively and automatically, as well as analysed by a computer program. In this article, information was sent via video

utilising the AES Algorithm using an image, audio, and video. The messages are encrypted and decrypted before being inserted in the cover picture. The AES algorithm is used in video steganography to transport information from one end to the other. Several methodologies and metrics may be measured objectively and automatically, as well as analysed by a computer program. In this study, information was sent via video utilising the AES Algorithm through image, audio, and video. The messages were encrypted and decrypted before being inserted in the cover video.

As an example of steganography, the project effort involved embedding text into video using the AES algorithm. The two fundamental criterion for effective steganography are that the stego signal produced by embedding is perceptually indistinguishable from the host video signal and that the embedded message is accurately retrieved at the receiver.

As demonstrated below, the suggested project is run in Apache NetBeans using the GUI.

Figure 1: Main page

Figure 1 is the main look of the project where one can encrypt/decrypt then embed/de-embed the files.

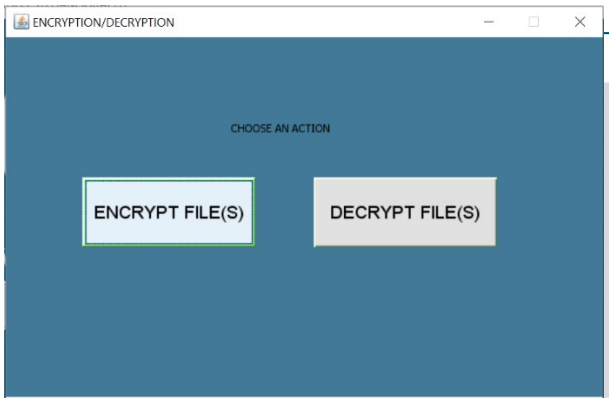

Figure 2: Encryption/Decryption

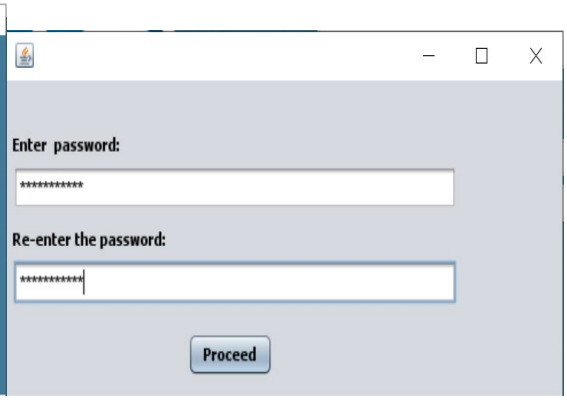

Figure 3: Key/Password

In figure 2 one can select the file they want to encrypt and then enter the key/Password in figure 3 to encrypt the file and in figure 4 one can see the encypted file.

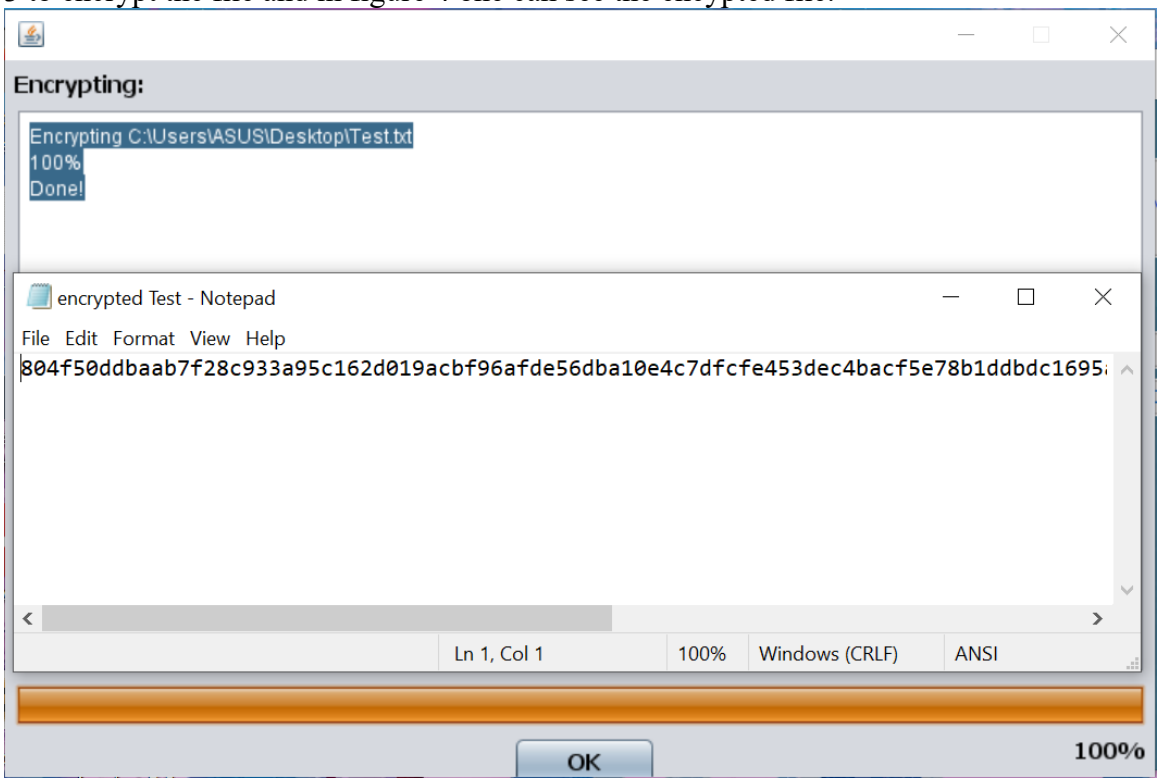

Figure 4: Encrypted file

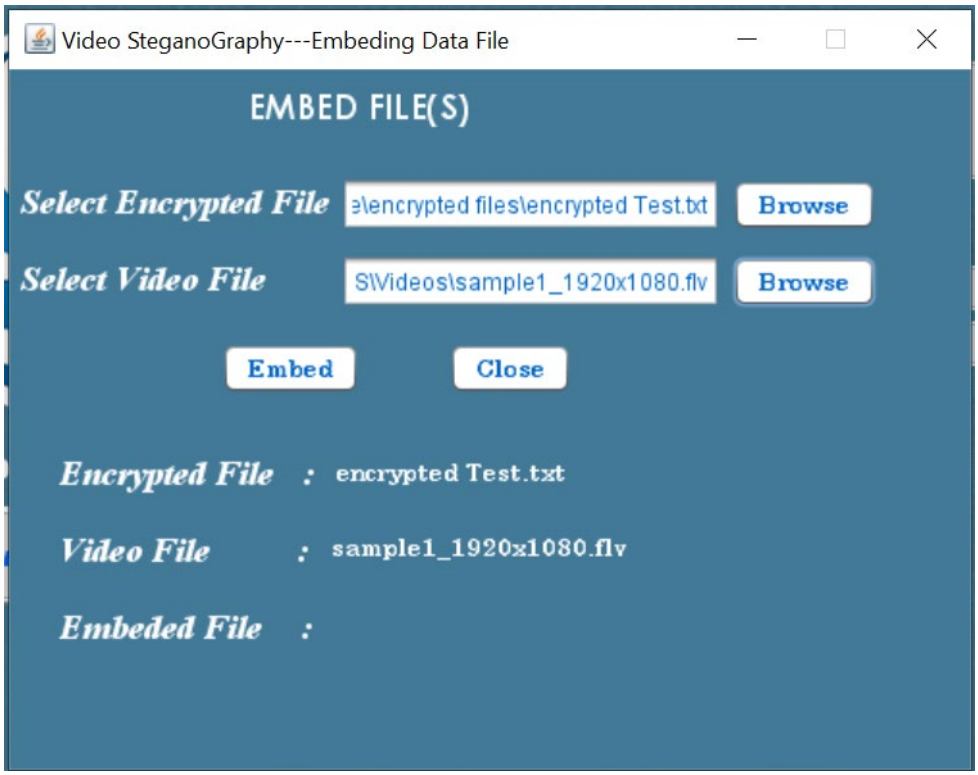

Figure 5: Steganography

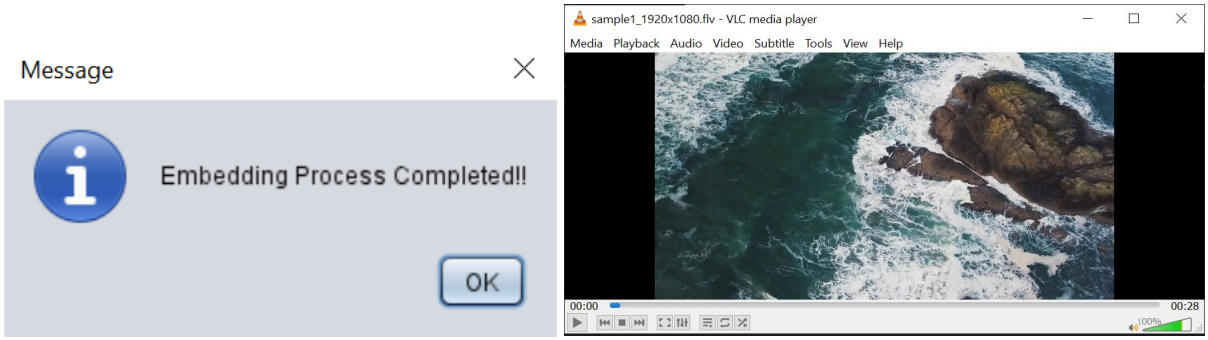

Figure 6: Steganography process

In Fig. 5 and 6 the input video and the media player are selected. The carrier video is chosen here, on which the secret text data is hidden and transferred via the channel.

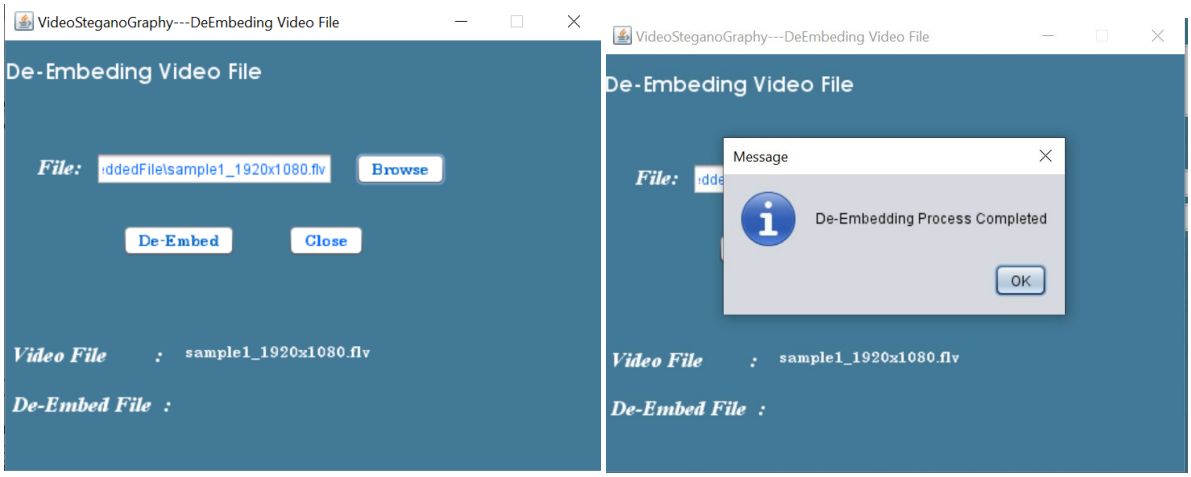

Figure 7: De-Embedding file

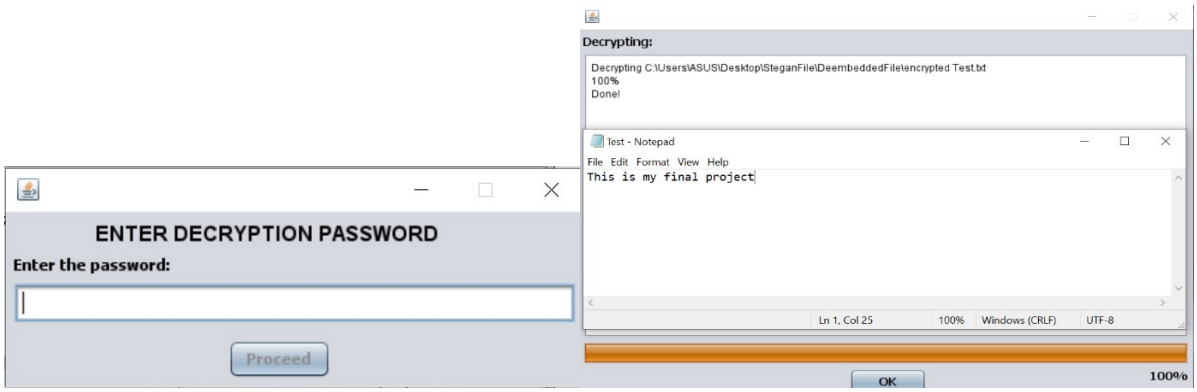

Figure 8: Decrypted file

Figure 8 shows the completion of the decryption process. The recovered data at the receiving end is identical to the original secret data presented in the figure.

A comparison of the proposed method with other video steganography techniques:

Studies	**PSNR (dB)**	**Payload (bpp/%)**	**MSE**	**Robustness**
The proposed method	**Best value = 82.02 average = 71.2878**	**For best PSNR value = 8.1% average = 14.25%**	**Best value = 0.00077 average = 0.9996**	**Not robust to compression and noise, but robust to physical operation and visual attack, providing more security.**
Kapoor & Mirza (2015)	Best value = 52.94	Average value = 2.66	Best value = 0.33	Not significantly robust to signal processing, noise, physical operation, statistical assaults, and compression.
Chitra & Thoti (2013)	Best value = 53.04	Average value = 2.66	Best value = 0.32	Not sufficiently robust to signal processing, noise, physical operation, statistical exploitation, and compression.
Gupta & Chaturvedi (2013)	Highest value = 49	Average value = 1	------	Not robust to signal processing, noise, physical operation, or compression, yet resistant to statistical exploitation.
Younus & Younus (2019)	Highest value = 67.3638	Average value = 2.92	Lowest value = 0.2578	Not enough robust to signal processing, noise, physical operation, statistical assaults, and compression.

Mstafa & Elleithy (2016)	Average value = 74.54	Average value = 1	------	Not enough robust to signal processing, noise, physical operation, statistical assaults, and compression.
Sadek, Khalifa & Mostafa (2015)	Average value = 54.64	Average value = 0.23%	------	Robust against the MPEG-4 codec
Khupse & Patil (2014)	Average value = 85.18	Low payload only frame is used (2120 bits per video)	------	Not enough robust to signal processing, noise, physical operation, statistical exploitation, and compression.

7 Conclusion and Future Work

This research looks at the fundamentals of steganography and cryptography, as well as its applications in the safe transmission of digital data over networks. The author provides a technical review of current cryptography and steganography technology. Combining these two operations has been found to be safer than performing them alone.
The AES method was used in the study (Ezhilarasi, 2019) to communicate secret information from the sender to the recipient using video. The AES algorithm was used to protect against both secure and resilient cryptographic assaults. Steganography is classified according to a number of variables, one of which being the cover material utilised. The term "video" refers to a collection of visuals mixed with sound. This category contains all videos that can be used for video steganography. This might be used in a security system as a future research topic.

Video Presentation Link:
https://studentncirl-my.sharepoint.com/:v:/g/personal/x20182457_student_ncirl_ie/EaaxXI1735lNgzZrq7yJsEwBxD4BuDP0Qzzvo6WF_v_lSw?e=jbwiel

References

Almuhammadi, S., 2020. *A SURVEY ON RECENT APPROACHES,* Saudi Arabia: College of Computer Sciences and Engineering.

AL-Shaaby, A., 2020. Cryptography and Steganography: New Approach. *SOCIETY FOR SCIENCE AND EDUCATION,* 5(6).
Beloglazov, A. & Buyya, R., 2015. Openstack neat: A framework for dynamic and energy-efficient consolidation of virtual machines in openstack clouds. *Concurrency and Computation: Practice and Experience,* 27(5), pp. 1310-1333.
Ezhilarasi, C., 2019. Video Steganography and Security Cryptography. *International Journal of Linguistics and Computational Applications,* 4(4).
Ezhilarasi, C., 2019. Video Steganography and Security Cryptography. *International Journal of Linguistics and Computational Applications,* Volume 04, p. 04.
Feng, G. & Buyya, R., 2016. Maximum revenue-oriented resource allocation in cloud. *International Journal of Grid and Utility Computing,* 7(1), pp. 12-21.
Gomes, D. G., Calheiros, R. N. & Tolosana-Calasanz, R., 2015. Introduction to the special issue on cloud computing: Recent developments and challenging issues. *Computer & Electrical Engineering,* Volume 42, pp. 31-32.
K.S. Seethalakshmi, U. B. a. S. K. N., 2016. *Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography.* s.l., s.n.
Kune, R. et al., 2016. The anatomy of big data computing. *Software—Practice & Experience,* 46(1), pp. 79-105.
M. M. Amin, M. S. S. I. M. R. K. a. M. Z. S., 2003. *Information hiding using steganography,* NCTT 2003 Proceedings., Shah Alam, Malaysia, Malaysia: 4th National Conference of Telecommunication Technology.
M. S. Shahreza, ". v. 4. 2., 2005. An Improved Method for Steganography on Mobile Phone. 4(4).
Madhusudan, V. S. a., 2015. *Two New Approaches for Image Steganography Using Cryptography,* s.l.: IEEE Int. Conf. Image Information Processing.
N. Patel, S. M., 2016. *LSB Based Image Steganography Using Dynamic Key Cryptography,* s.l.: in International Conference on Emerging Trends in Communication Technologies (ETCT).
Parik, H. & Amin, J., 2016. Data Compression and Steganography Using. *IJARIIE-ISSN,* 2(3).
R. Das, I. D., 2016. *Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques,* s.l.: in IEEE Int. Conf. on Research in Computational Intelligence and Communication Networks (ICRCICN).
S. Bukhari, M. S. A. M. A. a. S. D., 2016. *Enhancing security of images by Steganography and Cryptography techniques.* s.l., s.n.
Singhal, V. & Prakash, N., 2020. Image Steganography embedded with Advance Encryption Standard (AES) securing with SHA-256. *International Journal of Innovative Technology and Exploring Engineering,* 9(8).
Soe, W. W. Z. a. T. N., 2011. *Implementation and analysis of three steganographic approaches.* Shanghai, China, s.n.
Wagh, S. K., Upadhyay, G. & Bakan, U., 2020. Cryptography and Steganography Techniques in Video. *International Journal of Recent Technology and Engineering,* 9(2).
Wajgade, V. M. & Kumar, S., 2019. Enhancing Data Security Using Video Steganography. *International Journal of Emerging Technology and Advanced Engineering,* 3(4).
Yee, L. K., 2017. Secret Channel Using Video Steganography. *INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION,* 1(4).