GAZI UNIVERSITY

FACULTY OF ENGINEERING – COMPUTER ENGINEERING

171180010 – Cansu AYTEN

171180005 – Gamze AKSU

CENG482 INTRODUCTION TO COMPUTER SECURITY

TERM PROJECT: STEGANOGRAPHY TOOL

MAY 2022

CONTENTS

ABBREVIATIONS

Abbreviations	Descriptions
AR	Augmented Reality
ASCII	American Standard Code for Information Interchange
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DSSS	Direct Sequence Spread Spectrum
DWT	Discrete Wavelet Transform
EAS	Enhanced Audio Steganography
FFMPEG	Fast Forward Moving Picture Experts Group
GUI	Graphical User Interface
IDE	Integrated Development Environment
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
MP3	MPEG-1 Audio Layer III
OpenCV	Open Source Computer Vision Library
PIL	Python Imaging Library
RGB	Red-Green-Blue
RSA	Rivest-Shamir-Adleman
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAV	Waveform Audio File Format
XOR	Exclusive OR

ABSTRACT

The method that enables a message to reach the target without being noticed by third parties is called steganography. The difference of steganography from cryptography is that the message is made unreadable by using a key in cryptography, while the presence of the message is hidden in steganography. Three types of steganography techniques were developed within the scope of this project. These techniques can be listed as image, audio and video. There are many different algorithms for embedding messages in these steganography methods. The algorithm used for all three types in this project is the least significant bit algorithm. In the Least significant bit algorithm, the message is stored in the least significant bits of the file in which the message will be embedded. There is no doubt that there is a message in the file, which is obtained as an output, since there is no visible difference from the original version of the file with the message embedded in it. Steganography alone sometimes does not provide sufficient protection, so cryptography and steganography are used together. For this reason, messages within the project were encrypted using the RSA encryption algorithm before being integrated into the environment with steganography.

1. INTRODUCTION

Data security and privacy has been a major concern in the past and today. With the development of the Internet, information exchange and communication has become faster and simpler. However, the concern of data security and privacy has started to grow day by day. With digital advances, protecting sensitive information from outsiders such as hackers or intruders is a challenge. For this reason, some methods have been developed and started to be implemented in order to ensure information security and confidentiality. One of these methods is steganography.

The data sent from one place to another is encrypted to prevent others from seeing it and to provide confidentiality. With the use of a key in the cryptography technique, the message is rendered unreadable and sent. The decryption key is required to decrypt the message and make it meaningful. In steganography, unlike cryptography, the existence of the message must be hidden instead of hiding the content of the message. Thus, the message or its content cannot be accessed. When looking at an image, it is expected that people other than the person who sent the message in that image will not understand the existence of the message. Anyone who looks at the message other than the sent person cannot notice that there is another important information in the viewed image. Therefore, it does not attempt to seek any information. Steganography is used for this. Information is hidden inside information. Writing secret messages with invisible ink in a letter, and only the person who knows the way this ink will appear, can know the existence of this message and read the message, is a simple example of hiding information in information.

1.1 Scope

In this study, which we have done as part of the term project of the Introduction to Computer Security course, a Steganography tool including Image, Audio and Video Steganography has been developed. In this tool, a message can be hidden in image, audio and video. The presence of the message is not noticed in the printouts after it is hidden. However, after decoding, the message can be accessed.

The main purpose of this developed project is to establish a connection and ensure that the message reaches the target correctly, without the presence of the message being perceived by people other than the parties to communicate. While doing this, the change in the state of the environment that allows the message to be sent by embedding should be at a level that cannot

be noticed by people. In this way, the confidential communication to be made will not attract suspicion and the message will be shared secretly.

2. A BRIEF HISTORY OF STEGANOGRAPHY

Throughout history, information hiding methods have been used for many purposes. Examples of these are political or diplomatic negotiations, pre-war preparations, wars, espionage activities, etc. can be given. [1]

When the steganography examples in the past are examined, the story of Herodotus comes to mind first. Herodotus engraved the rebellion message he would send during the Persian attack on the head of one of his slaves. When the slave's hair grows, the message is hidden. In this way, he sent the message without attracting attention. When he went to the person to whom he would give the message to the slave, he asked him to shave his head. In this way, the message reached its destination.

Wax tablets were widely used in ancient Greece. Messages were written on the wooden part of the wax tablets. These messages were hidden by covering them with wax. These tablets looked like an unused wax tablet at first glance, but when the wax on it was melted, it was understood that the tablet contained a message. Thus, the secret message could be read.

In the Second World War, steganography examples are seen more often with the effect of the war. In the war between the French and the Germans, both sides provided messaging with invisible inks. That's why people were trying to develop new invisible ink formulas to reveal the messages of their enemies. Similarly, during the Second World War, the Japanese national agent hid in New York in disguise. He was sending the letters he was going to send, disguising them as business letters.

There were sprays and pens containing ultraviolet dye that were popular in the 1960s. Messages written with these sprays and pens could only be viewed under ultraviolet light.

In A Beautiful Mind, a 2001 movie directed by Ron Howard, it is seen that John Nash, a mathematician, searches for hidden messages in newspapers and magazines.

3. LITERATURE REVIEW

While steganography is being done, storing the message alone does not always protect the message. For this reason, sometimes the messages are encrypted with cryptography and then stored with steganography, increasing the security of the message.

Singh et al (2015) used the least significant bit algorithm to hide messages in image files.

Bhuiyan et al. (2019) used an LSB algorithm developed into image files to hide messages in their study. They XOR the bits of the message with the 7th bit of the image, and then the output produced is embedded in the 8th bit of the image.

Fatma and Nurul (2018) embedded the messages in the audo files using the LSB algorithm. The study only supports .wav files.

Sinha et al. (2015) first encrypts the message with the Vigenère encryption algorithm and then embeds the message in the audio file using the LSB algorithm

Satam et al (2013) performed Audio in Audio steganography, Image in Audio steganography, and Audio in Image steganography using LSB, DCT and DWT methods.

Younus and Younus (2019) embed messages in video files by using Knight Tour Algorithm and LSB Method in their work. They worked on .avi files.

BanuPriya et al. (2019), in their work, the message is first encrypted with RC7 Encryption. The message is then embedded in the video using the LSB algorithm. Finally, the video is encrypted using the Chaos Encryption algorithm.

4. METHODOLOGY

4.1. Steganography

Steganography ensures that the existence of a sent message is not suspected by anyone other than the sender and receiver, thus ensuring the confidentiality of the communication. Messages are hidden inside other files without changing their structure. For example, hiding messages in other texts, images, sounds and videos. Here there is no difference between the original file and the file with the message hidden in it. The existence of a secret message cannot be understood when looking at the file containing the secret message.

Cryptography and steganography are very similar. The purpose of both is to protect information, but the methods used are different. In cryptography, the message is hidden by

making it incomprehensible, while in steganography the existence of communication is hidden. In cryptography the data is visible but unreadable whereas in steganography the message is not. While the general structure of the data is changed in cryptography, it is not changed in steganography. In cryptography a key is required to encrypt the message whereas in steganography the key requirement is optional. In cryptography, the decryption key is needed to convert the encrypted message to the original message and thus learn the message. In steganography, once the existence of this message is understood, the data in the secret message becomes available to everyone.

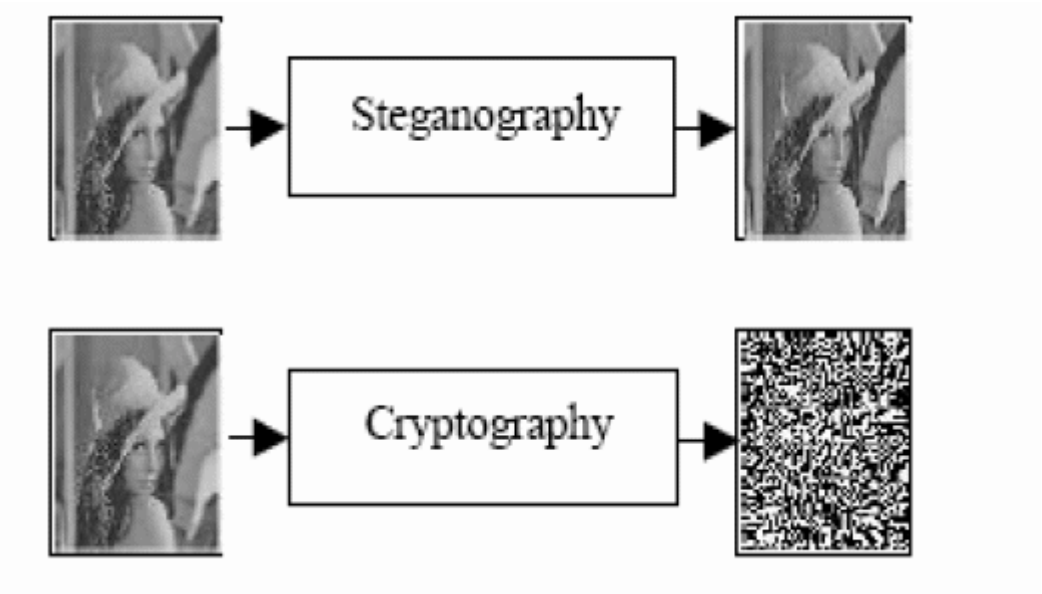

Figure 1: Steganography vs Cryptography

4.2. Steganography Techniques

There are many objects in which secret messages can be embedded. In this respect, steganography can be divided into five types: Text Steganography, Image Steganography, Video Steganography, Audio Steganography and Network Steganography.

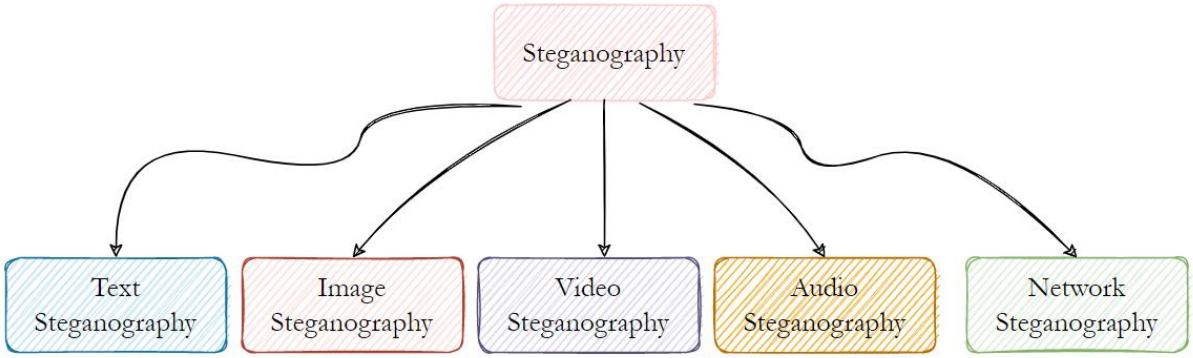

Figure 2: Steganography Techniques

4.2.1. Text Steganography

The method in which the message is hidden in a text is called text steganography. In this method, the format of the text can be changed, the words in the text can be changed, random character sequences can be created and many other ways of hiding can be performed. The simplest way of use can be given as an example of hiding the message to the first letter of each word in an article or to the first letter of each sentence in a poem. Text steganography is more difficult than others as the size of the text file is smaller than image, audio or video files. Files such as images, audio, and video are large in size, so changes are too small to be noticed in the output. But a change made to hide a message in a text file can be easily understood by anyone. Text steganography methods can be explained under three headings: Format Based Methods, Random and Statistical Generation and Linguistic Steganography.[9]

4.2.1.1. Format-Based Methods

In format-based methods, it is physically changing the format of the text to hide the massage in the text. Physical alteration of the text may arouse suspicion for readers. When the file with the text hidden inside is opened with a word processor, additional spaces in the text, spelling mistakes, and capitalization changes are seen. In addition, when the original plain text is reached, the hidden message is revealed by looking at the differences.

4.2.1.2. Random and Statistical Generation

In this method, stagnographers create their own text files so that there is no match to a known plain text. Steganographers use this method to produce words that will have statistical properties similar to real words in a given language, statistical properties of word length and letter frequencies to hide text within text.

4.2.1.3. Linguistic Steganography

The mechanism of the language is used to hide the text, taking into account the characteristics and linguistic features of the language in which the text is written. Since the text is encrypted using grammar in this method, although the text is grammatically perfect, there are semantic defects in the text. In addition, a little grammar in this method sometimes leads to text repetitions.

4.2.2. Image Steganography

Image steganography is the hiding of a message such as text or sound inside the image. Since an image consists of pixels (bits), these pixels are used in steganography. Steganography is performed by hiding the messages between the pixels of the image. With the message hidden between the pixels, there is no visible difference between the original image and the steganographic image.[10]

Least significant bit, masking and filtering, algorithms and transformation methods can be used in image steganography.[11]

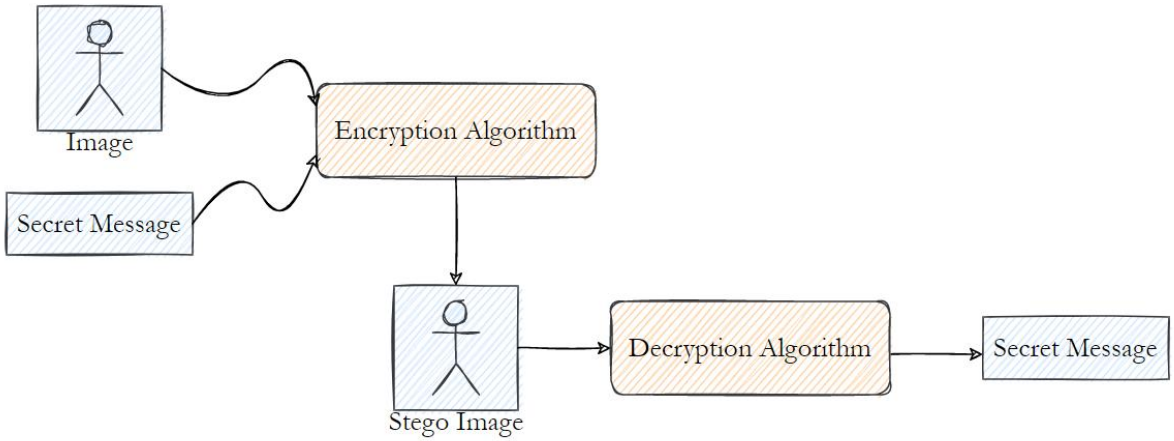

Figure 3: Image Steganography

4.2.2.1. Least Significant Bit

One of the most basic methods in the field of steganography is the Least Significant Bit (LSB) algorithm. In this algorithm, the message to be hidden in the image is first made into binary. The binary message is embedded in the least significant bit of the bits in the image. In this algorithm, the bits to hide the message are selected sequentially, not in a different way. Therefore, a sign is added at the end of the message to indicate the end of the message, as it cannot be understood when the message is finished. Color images (RGB) have 3 different channels. Messages can be embedded in any one of these channels or in all three of them sequentially.

Gömülecek Bitler	1	1	0	0	1	1
Resme Ait Bitler	01000010	11111101	11100111	01100001	01101011	00101010
Sonuç	01000011	11111101	11100110	01100000	01101011	00101011

Figure 4: Example of bit embedding [12]

For an image represented by 8 bits, each bit of the image ranges from 0 to 255. Therefore, as a result of a change in the least significant bit, that is, the eighth bit, changes occur in the image that is too small to be noticed by the human eye.

Decryption process is applied to read the message in the image. In the decryption process, the reverse of the message embedding process is performed. A message is created by combining the values in the least significant bit of each pixel in the image.

4.2.3.2. Masking and Filtering

The message hidden in an image is masked by a faded image. In this way, messages are hidden inside the image so that the human eye cannot see them. The masking method is better for use with JPEG images. Because it is resistant to condensation and clipping.

4.2.3.3. Algorithms and Conversion

Different transformation algorithms can be used to embed the message in the image. Frequency transformations such as Discrete Fourier Transform, Discrete Cosine Transform, Discrete Wavelet Transform are examples of these transformation algorithms.

JPEG uses the Discrete Cosine Transform to achieve compression. Rounding errors occur frequently when calculating cosine values. Therefore, the cosine values cannot be calculated exactly. Therefore, the Discrete Cosine Transform method is a lossy transformation. Depending on the approach and values used, the results will differ.

4.2.3. Audio Steganography

In the sound steganography method, the message is hidden in an audio signal. The human ear cannot distinguish the changes in the new sound file. Therefore, anyone who does not know that there is a secret message in this audio file cannot access the secret message. It is more difficult to hide a message in audio media than to hide a message in video media. WAV, AU and MP3 audio files can be hidden with audio steganography technique.

Methods such as Least Significant Bit Encoding, Parity Encoding, Phase Coding, Spread Spectrum and Echo Data Hiding can be used in audio steganography. [13]

4.2.3.1. Least Significant Bit Encoding

It is the simplest method in audio steganography. A binary message is replaced with the least significant bits of the audio file. The transfer rate depends on the channel capacity. It is 1 kbps per 1 kHz. When having a 6 kHz array, the capacity would equal 6kbps. Large amounts of data can be encoded with this method. But LSB is vulnerable to manipulation. The fact that a large amount of data can be processed into the audio file also increases the noise generated. If the length of the message to be encoded in audio steganography is less than the total number of samples in the audio file, subset selection should be made for the samples that will transmit the message to the user.

Some changes can be made to the LSB method in order to increase security. Because although the LSB method has low computational load and simplicity, it is insufficient in terms of security. This situation can be overcome with Enhanced Audio Steganography (EAS), which has more layers of encryption and decryption. In this technique, the message is first encrypted and then hidden.

4.2.3.2. Phase Coding

The original audio file is split into short segments. DFT (Discrete Fourier Transform) is applied to each segment and then the phase difference is calculated for each. After calculating the phase difference for all segments, new phase frames are created. The phase and original magnitude are connected to make a new segment. All segments are interconnected for convenient ecrypted output.

4.2.3.3. Spread Spectrum

The message is encrypted with the help of a cryptographic algorithm. Afterwards, the message is embedded in the original audio using the Direct Sequence Spread Spectrum (DSSS) method.

In Direct Sequence Spread Spectrum, the signal is multiplied by a pseudo-random sequence of a certain maximum length known as a chip.

4.2.3.2. Echo Data Hiding

The data is hidden to the signal with the use of echo. By adding echo to the signal, the data is embedded in the audio signal. This is done by changing the original amplitude, decay cost and offset or delay fields of the echo. As the offset develops, the echo and the signal mix. The human ear cannot distinguish this at a certain point and the echo is heard as extra resonance. The desired bits are encoded into the signal by dividing the echoing into smaller bits. The last echoed signal is a recombination of all independent echoed areas.

4.2.3. Video Steganography

In the video steganography method, the message is hidden in the videos. It can be said that the video steganography method is a combination of sound steganography and image steganography methods. As in these two methods, the message can be embedded in large amounts of data. Messages hidden in large amounts of data occupy a small area. Therefore, it cannot be noticed by people that there is a message in the video containing the secret message. Because the video looks exactly the same as the original. Apart from that, it has an animated audio and video stream.

There are two different ways to follow the steganography in the video. The first is to embed the message in the uncompressed raw video and then compress the video. The other is to embed the direct message into the compressed video stream.

4.2.4. Network Steganography (Protocol Steganography)

The Network Steganography method ensures that confidential messages go undetected while being transmitted over an insecure network. It uses legitimate traffic for this. Messages are embedded in protocols such as TCP and UDP used in data transmission. For example, hiding the information in the header of the TCP/IP packet can be given. [14]

4.3 Areas Where Steganography Is Used

Hackers use steganography methods when attacking. Hackers normally embed their malware inside seemingly safe files. One of the techniques they use is the LSB technique. Hackers identify the least significant bits in the carrier and embed the secret message within these bits. This process can be used with downloadable files or images. Another method used is called safe cap selection. In this method, hackers try to choose the most secure cover image for the

message to be stored. To do this, they compare the blocks of the image with the blocks of their messages and choose the one with the most matches. [15]

Software created by hackers is often malicious. When interacting with these software, the program comes to life even if it is not understood that the attack has taken place. There are many different ways hackers can reach their victims. The first of these is digital media files. They can embed malware in a photo on a website or in an email signature. In another method, hackers impersonate a legitimate website. Any interaction with this website results in the downloading of malicious software. In another example, it is used to obscure command and control traffic.

Apart from these, some different usage areas are listed below: [1]

- Some modern printers, including color laser printers from some brands, use steganography. Printers have been known to add hard-to-see little yellow dots to every page. Dots represent printer serial numbers, date and time.
- Steganography has historically been popular with agents. Illegal agents disguise and act as someone else by entering different countries and companies. During the spying, they communicated by hiding secret messages with steganographic methods. Hidden messages are embedded in files such as images, sounds or video.
- Steganography can also be used in games. Steganography and cryptography are used together in the puzzles offered by Cicada 3301. Puzzles containing steganography can also be used in AR games.

4.3.1 Steganalysis

Steganalysis is used to detect the presence of a hidden message in a file. Steganalysis methods used against image steganography are: [16]

- Visual Detection: It is called visual detection of some anomalies that occur as a result of data embedding in images.
- Histogram Analysis: This method is based on the statistical analysis of the changing pixel value pairs as a result of data embedding in the image.

- High-Order Statistical Analysis: In this method, in addition to the histogram analysis, statistical analysis of the positions of the pixels where the change takes place is also performed.
- Algorithm or Type-Specific Detections: It includes steganalysis methods developed specifically for image types with extensions such as JPEG.
- Universal Detection Systems: The features of the image are extracted and compared with the original image.

4.4 Platforms and Technologies

For the Steganography tool project, the Python programming language and the Spyder IDE were used. The tkinter library was used for the interface operations in the project. PIL library for image steganography, wave library for audio steganography and OpenCV and FFMPEG libraries for video steganography were used.

4.5 Methods Used In the Project

4.5.1 RSA

RSA algoritması asimetrik bir kriptoloji algoritmasıdır. Asimetrik çalıştığı için Public Key ve Private Key olmak üzere iki farklı anahtar kullanır. Public key herkes tarafından bilinirken, private key sadece mesajı yayınlayan kişi tarafından bilinir. Bu algoritmada p ve q olmak üzere iki adet asal sayı seçilir. Bu iki asal sayının çarpımı n değerini verir. Her ikisi asal sayının bir eksiğinin çarpımı ile totient değeri elde edilir. Public key e ise 1 ile totient değeri arasından seçilen bir asal sayıdır. Private key ise d*e = 1 mod (n) denkleminden çıkarılır. [17]

4.5.2. Steganography Types

Three different types of steganography were applied in the developed steganography tool. These are Image Steganography, Audio Steganography and Video Steganography. Least Significant Bit method was used for all three types. Messages are embedded in the selected file with the LSB method. If there is a message in the file selected with the decode operation, this message is revealed.

Before starting the steganography process, the first embedded message must be converted to bits. Each letter is converted to ASCII code so that the message becomes a number. The message is then encrypted with the RSA algorithm. Each letter of the encrypted message is then converted into bytes of 8 bits.

4.5.2.1 Image Steganography

In the scope of Image Steganography, all images are converted to RGB. The message is then sequentially embedded in the least significant bit within the 3 channels. In the decode operation, the reverse of the encode operation is applied. Letters are created by combining the values in the trivial bit by going to the 3 channels in the image sequentially. The generated letters are decrypted with the RSA algorithm and the message is revealed.

4.5.2.2 Audio Steganography

The frames in these audio files are converted to binary. Then, by applying the LSB technique to these binary values, the message is embedded by changing the least significant bit. Likewise, in the decoding process, the audio file is converted into frames, and the secret message is reached by combining the values in the least important bit in these frames. Only .wav files are supported under Audio Steganography.

4.5.2.3 Video Steganography

Within the scope of Video Steganography, the audio is separated from the video and the video is divided into frames. Thus, since there are two different file types as sound and image, steganography techniques of these file types can be used. While video steganography is being performed, the message can be embedded in images if desired. Image steganography techniques are used to embed the message in images. Likewise, if desired, the message can also be embedded in audio files. Audio steganography techniques can also be used to embed the message in audio files. For example, LSB technique is a technique that can be used in both audio and video steganography. In video steganography, messages are embedded in frames or sound with LSB technique. Then these frames and audio are combined into a video. As another example, with methods such as phase coding and echo hiding, which are mentioned in sound steganography, the message is hidden in the sound and a video is created by combining the steganographic sound with the frames. Similarly, the message can be hidden inside the frames. This message is turned into a video by combining the hidden frames.

4.6. GUI

GUI allows users to interact with the application. While designing the interface, it was given importance to be user-friendly. That's why the interface is designed to be uncomplicated, self-

explanatory, and easy to use. In Figure 4, there is the main page of the Tool. Here, the text to be hidden is entered and the desired steganography type is selected and proceeded.

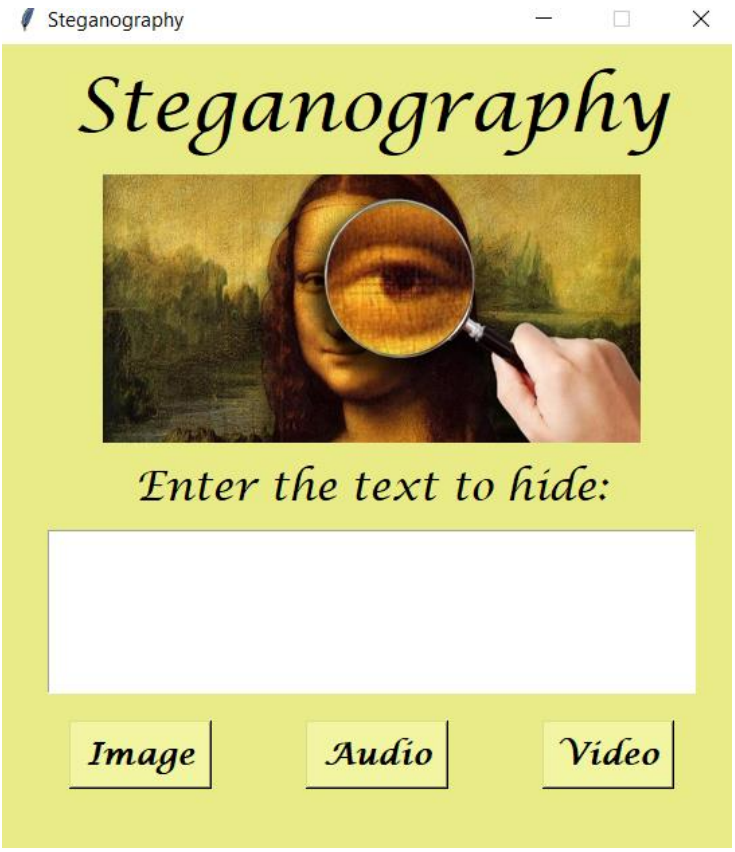

Figure 5: Steganography Tool Homepage

4.6.1 Image Steganography GUI

Image steganography page is given in Figure 5. After entering the message on the main page, clicking the "Encode" button on the Image steganography page opens a new page. This new page created for the encode section is given in Figure 6. On this page, there is a "Choose Image" button for image selection and a "Back" button that allows us to return to the homepage. After the image is selected, the entered message is embedded in the selected image. When the Decode

button is clicked, the message in the selected image is revealed. This message is presented to the user in a MessageBox. Figure 7 shows the page created for the decode operation.

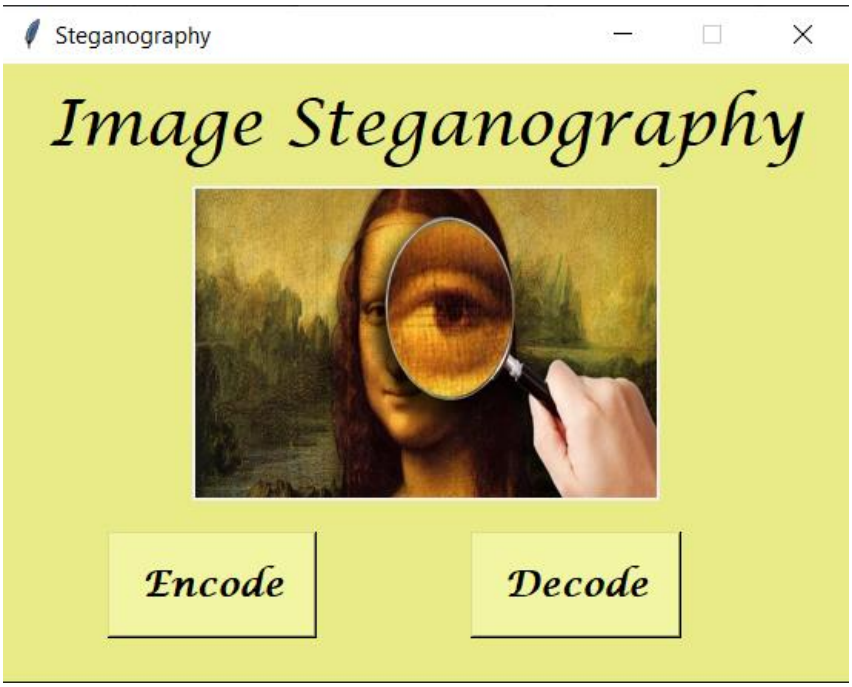

Figure 6: Image Steganography Page

Figure 7: Image Steganography Encode Page

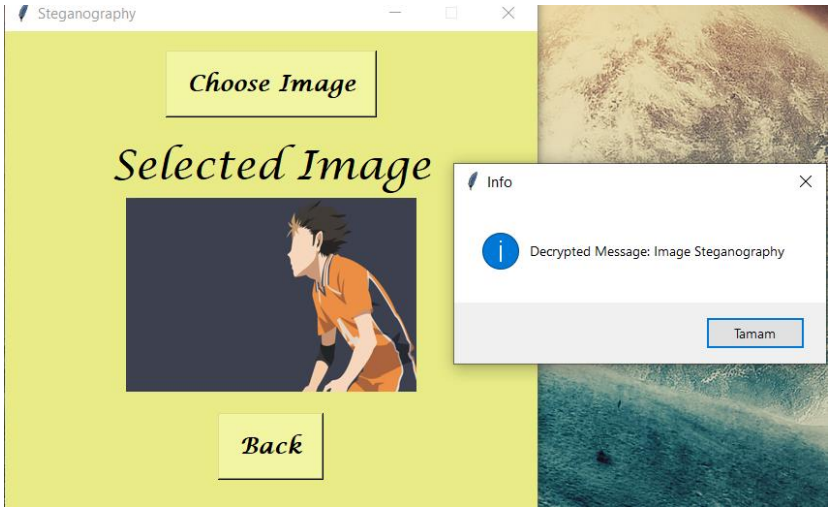

Figure 8: Image Steganography Decode Page

4.6.2 Audio Steganography GUI

Audio steganography page is given in Figure 8. After entering the message on the main page, clicking the "Encode" button on the Audio steganography page opens a new page. This new page created for the encode section is included in Figure 9. On this page, there is a "Choose Audio" button for the audio selection process and a "Back" button that allows us to return to the homepage. Apart from that, there are buttons on the page that allow you to play and stop the selected audio and encoded audio. After selecting the audio, the entered message is embedded in the selected audio. Clicking the "Decode" button reveals the message in the selected audio. This message is presented to the user in a MessageBox. As in the Encode page, there are two buttons to play and stop this audio. Figure 9 shows the page created for the decode operation.

Figure 9: Audio Steganography Page

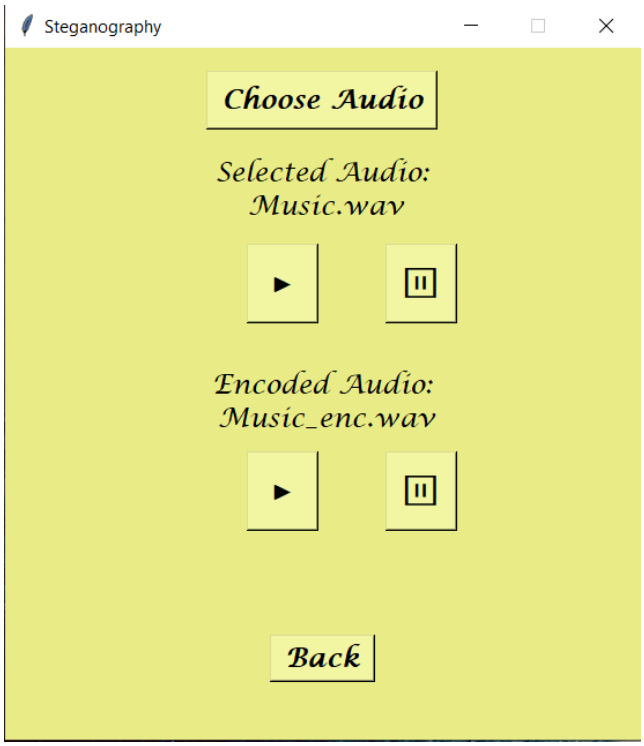

Figure 10: Audio Steganography Encode Page

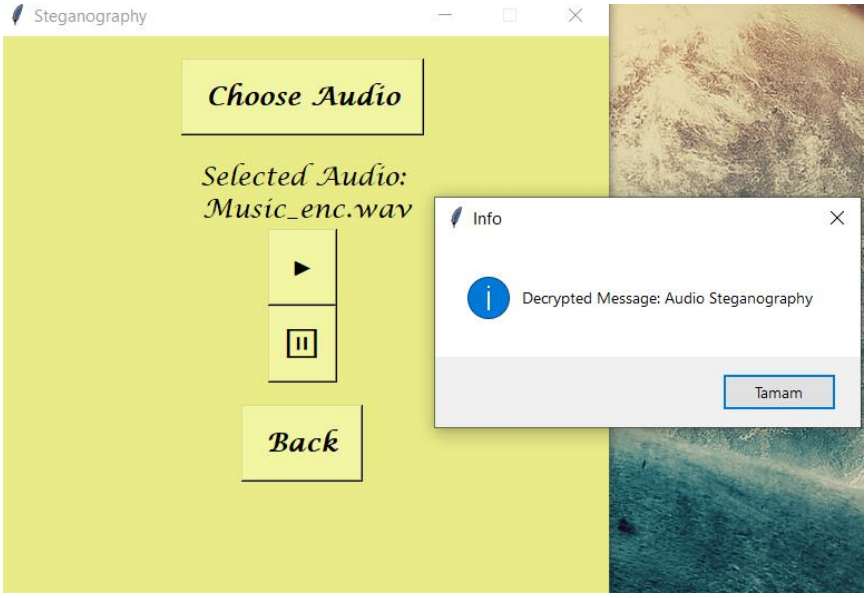

Figure 11: Audio Steganography Decode Page

4.6.3 Video Steganography GUI

Video steganography page is given in Figure 11. After entering the message on the main page, clicking the "Encode" button on the Video steganography page opens a new page. This new page created for the encode section is given in Figure 12. On this page, there is a "Choose Video" button for the video selection process and a "Back" button that allows us to return to the homepage. After the video is selected, the entered message is embedded in the selected

video. When the Decode button is clicked, the message in the selected video is revealed. This message is presented to the user in a MessageBox. Figure 13 shows the page created for the decode operation.

Figure 12: Video Steganography Page

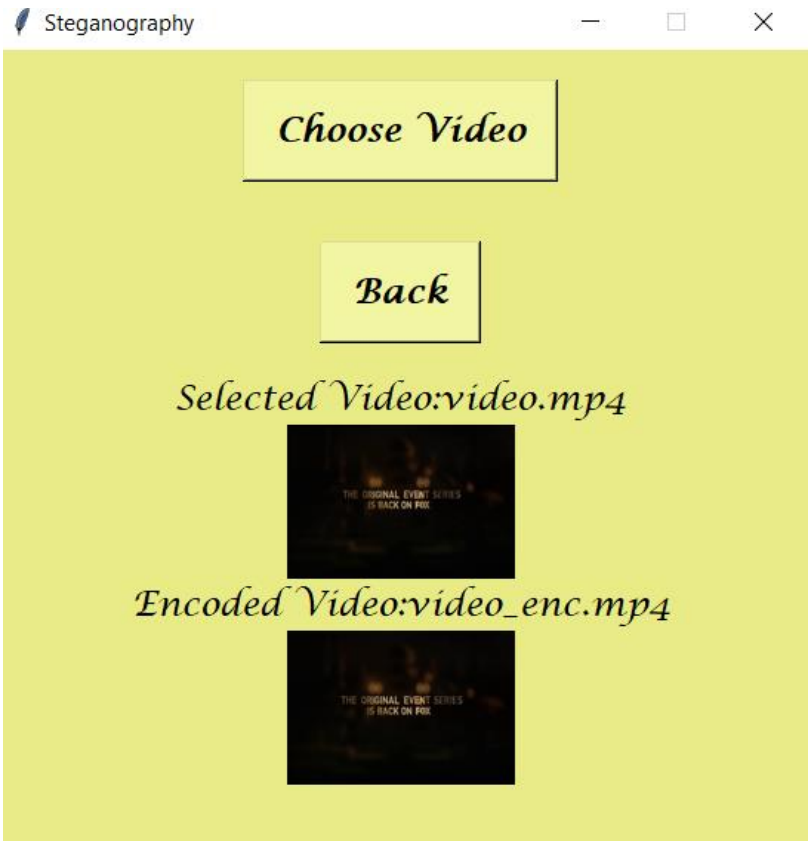

Figure 13: Video Steganography Encode Page

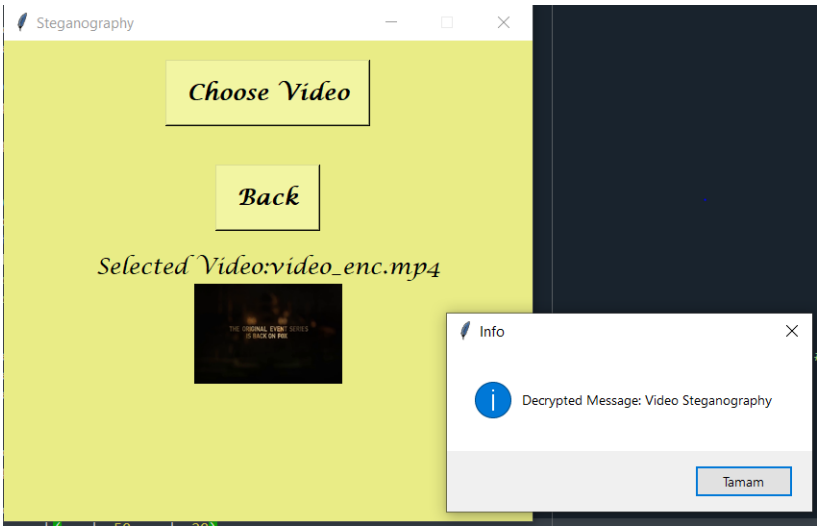

Figure 14: Video Steganography Decode Page

5. CONCLUSION

Steganography is simply hiding a file inside another file. Steganography is a form of covert communication. Any medium can be used to hide messages. However, steganography is not an encryption method. In steganography, messages are not encrypted. Steganography types are divided into five according to the environment in which the messages are hidden: Text Steganography, Image Steganography, Audio Steganography, Video Steganography and Network Steganography. In this project, Image Steganography, Audio Steganography and Video Steganography processes were carried out. A text message is embedded in image, audio and video files. The least significant bit technique, which is the simplest and fastest technique, is used to make image, audio and video steganography. A weakness of the Least significant bit method is that the message can be detected easily if the presence of the message is suspected. Therefore, in order to strengthen the confidentiality of the message, the message was encrypted with the RSA algorithm, which is a cryptographic algorithm, before the steganography process.

REFERENCES

1. Wikipedia contributors. (2022, May 6). Steganography. In *Wikipedia, The Free Encyclopedia*. Retrieved from https://en.wikipedia.org/wiki/Steganography
2. Singh, A., Singh, J. Singh, H. (2015). Steganography in Images Using LSB Technique
3. Bhuiyan, Touhid & Sarower, Afjal H. & Karim, Md Rashed & Hassan, Md Maruf. (2019). An Image Steganography Algorithm using LSB Replacement through XOR Substitution.
4. Mohamad, Fatma & Yasin, Nurul. (2018). Information Hiding Based on Audio Steganography using Least Significant Bit. International Journal of Engineering & Technology. 7. 536. 10.14419/ijet.v7i4.15.28363.
5. Sinha, N., Bhowmick, A., & Kishore, B. (2015). Encrypted information hiding using audio steganography and audio cryptography. International Journal of Computer Applications, 112(5), 49-53.
6. Chadha, A. Satam, N. Sood, R. Bade, D. (2013). An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution https://arxiv.org/ftp/arxiv/papers/1311/1311.1083.pdf
7. Younus, Z. Younus, G. (2019). Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data. Retrieved from https://www.degruyter.com/document/doi/10.1515/jisys-2018-0225/html
8. R. BanuPriya, J. Deepa, S. Suganthi, Video Steganography Using LSB Algorithm for Security Application, International Journal of Mechanical Engineering and Technology 10(1), 2019, pp. 203 211.
9. What is Text Steganography in Information Security? (2022). Retrieved From https://www.tutorialspoint.com/what-is-text-steganography-in-information-security
10. What is Image Steganography in Information Security? (2022). Retrieved from https://www.tutorialspoint.com/what-is-image-steganography-in-information-security#
11. What are the methods of Image Steganography in Information Security? (2022). Retrieved from https://www.tutorialspoint.com/what-are-the-methods-of-image-steganography-in-information-security
12. Demirci, B. (2016). GÖRÜNTÜ STEGANOGRAFİ MEDOTLARI VE PERFORMANSLARININ KARŞILAŞTIRILMASI.

13. What are the methods of Audio Steganography? (2022). Retrieved From https://www.tutorialspoint.com/what-are-the-methods-of-audio-steganography
14. Choudary, A. (2022). Steganography Tutorial – A Complete Guide For Beginners. Retrieved From https://www.edureka.co/blog/steganography-tutorial
15. Steganography: What Is It and How Does Steganography Work? (n.d) Retrieved From https://www.okta.com/identity-101/steganography
16. Hassan, M. (2008). STEGANALİZ YAKLAŞIMLARININ KARŞILAŞTIRILMASI
17. Duvan, İ. (2019). RSA Algoritması Nedir? Nasıl Çalışır? Retrieved From https://medium.com/@isaduvan/rsa-algoritmas%C4%B1-nedir-nas%C4%B1l-%C3%A7al%C4%B1%C5%9F%C4%B1r-bc351e63364c