

Enhancing Data Security Using Text Cryptography and Multimedia Steganography

MSc Research Project
Cyber Security

Pooja Vinod Paniker
Student ID: x20218966

School of Computing
National College of Ireland

Supervisor: Prof. Vanessa Ayala-Rivera

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Pooja Vinod Paniker
Student ID: x20218966
Programme: MSc Cyber Security **Year:** 2021-2022
Module: MSc Internship
Supervisor: Vanessa Ayala-Rivera
Submission Due Date: 31/01/2022
Project Title: Enhancing Data Security Using Text Cryptography and Multimedia Steganography

Word Count: 4473 **Page Count:** 17

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: Pooja Vinod Paniker

Date: 31/01/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

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

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

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

Enhancing Data Security Using Text Cryptography and Multimedia Steganography

Pooja Vinod Paniker
x20218966

Abstract

Data concealment is an important task that must be undertaken to preserve the quality and protection of information being conveyed and to avoid data tampering. Cryptography and steganography cannot be alone used to protect data, rather they can be combined and used in a single system. This paper aims to keep the information secured from third-party users who might mistreat them. This paper provides a solution to create efficient information masking to safeguard and protect data delivered. AES encryption and LSB are two of the significant methods of data encrypting and hiding used in the presented work. The suggested technique offers a method that combines the two different data hiding approaches into a unified system to provide improved data security. By encrypting data first and then hiding the encrypted data within an image or audio file, this integration of the two approaches improves data security. The results obtained from this work produced a high-quality standard stego image/ audio. To analyse the results of project PSNR and MSE value of the stego image/ audio are evaluated, the obtained metrics from the evaluation suggest that the system produces a high-quality stego image and stego audio.

1 Introduction

Despite substantial research into secure data exchange, an intruder could discover new ways to get sensitive data. A practical approach should be invisible, long-lasting, capable of carrying a substantial payload, and quiet. As technology advances, users face numerous data security, data confidentiality, privacy, and security challenges. The users are briefed ahead of time regarding the secrecy of their data, whether for cloud deployment or data transmission, yet there is a risk of a data breach in specific ways. The privacy and security of data communicated through the internet are insufficient, and an unauthorized user can intercept them. As a result, ensuring data transfer security and confidentiality is a significant and relevant necessity. Various methods, including Steganography and Cryptography, can be used to meet this condition (Alam, et al., 2013).

According to studies, cryptography and steganography appear to be among the most significant methods for data security. Cryptography is essential for turning raw data into an encrypted format, which is incomprehensible to individuals. Techniques of cryptography can be classified into two groups: Asymmetric-key cryptography and symmetric-key cryptography. In symmetric key, both the sender and receiver use the same key. Asymmetric key employs two distinct keys: a public key that anybody can see, and a private key that only the data recipient knows (Raphael & Sundaram, n.d.).

Steganography and cryptography are both used to protect sensitive information. The difference between the two is that Steganography entails hiding data in a manner that looks there is no data hidden at all. The process of embedding data into another digital medium without disclosing the data within the medium is known as steganography (Gautam, 2019). Although cryptography and steganography provide some data protection, this research proposes combining the two technologies into a unified system to protect secret information. There are two levels of data protection in this system. For both picture and audio steganography, the encrypted data is concealed inside an image or audio file using the Least Significant Bit (LSB) technique after encrypting the text .

Research Question: Will the concatenation of data concealing techniques cryptography and steganography in a single system be offered to enhance or safeguard the data of the user? What can be done to boost the secrecy of any user's private data?

The primary motivation of this research report is to find how cryptography can be made less vulnerable by combining it with steganography. Data security is improved by the proposed concept. This work has also looked into the ideas of secrecy and integrity and offers a suitable solution to improve the quality of the stego image/ audio. The integration of the two techniques will eventually aid in the secure exchange of data.

The work presented in this paper is further built on previous research work (Paniker, et al., 2020), this paper is taken as a base paper to carry out further research and improvements. While the earlier work focuses on only the properties changes of the original data and the final data, this research paper focuses more on evaluating the image quality and signal quality of the audio/ video after performing the proposed approach by comparing the Peak signal-to-noise ratio (PSRN) and Mean squared error (MSE) values of the final carrier medium. Further, improved results and detailed comparisons eventually support the motivation to decrease the vulnerabilities and strengthen the proposed method (Paniker, et al., 2020).

2 Related Work

This section gives an overview of the similar work that has already been implemented previously. The literature review is done on the two methods that are utilized in the prototype. This literature study has evaluated and assessed past study approaches on Advanced Encryption Standard (AES) and Least Significant Bit (LSB) algorithms. Because audio steganography is frequently utilized and among the most prominent steganographic methods, the human auditory system is hypersensitive to slight disturbances within audio signals, making it ideal for hiding data in audio files, according to studies.

2.1 Advanced Encryption Standard

To justify the use of the Advanced Encryption Standard (AES) algorithm in this prototype is that, as it can be used across both software and hardware its security standards are most secured, and for the encryption process, this algorithm also employs a key size of higher length which makes it difficult for the hackers to crack it (Sousi, et al., 2020). One of several primary issues of any digital information is secure. The authors of "AES Hybridization with Genetic Approach for Guarded Image Transmission" (Bindra & Bawa, 2018) developed a unique method for increasing the safety and secrecy of data by combining cryptography with steganography. Authors used the Advanced Encryption Standards (AES) technology to encrypt the data, which was then used to create an image via a genetic approach (Bindra & Bawa, 2018). The researchers noticed that by using the proposed integrated strategy, they were capable of improving the confidence and privacy of the digital data sent. To safeguard the secrecy of information, a variety of encryption methods are known, which are selected depending on the needs of the users. The researchers (Semwal & Sharma, 2017) examine and contrast several cryptography methods in respect of characteristics and efficiency expense to establish the best approach for certain activities. AES, ABE, Blowfish, CAST128, DES, 3DES, and IDEA were the algorithms used. Key size, frequency of rounds, frame size, multiple susceptible assaults and level of security were all used to produce a comparison study. The findings of this research show that every one of the strategies has its own set of qualities and shortcomings. These were selected depending on the needs of the customer (Semwal & Sharma, 2017). Since the AES encryption provides the maximum avalanche impact, it's appropriate for applications that prioritize secrecy and reliability (Semwal & Sharma, 2017). A study (Sheth & Saxena, 2016), explains a type of steganography in which data is hidden within a picture. Each picture byte's bottom nibble is updated to contain each nibble of the input sentence. This implementation's steganography method maximizes data storage while still ensuring security. The Java programming language is popular because of its large library of functions and simplicity of usage. The AWT and SWING libraries in Java were used to create a rudimentary GUI. The AES encryption method is also utilized to improve the program's security.

2.2 Least Significant Bit

The least significant bit of the picture is substituted with data bits in this approach. The research paper by (Alam, et al., 2013) has conducted research that shows by utilizing the Least Significant Bit (LSB) algorithm, can improve the quantity of message or secret data that can be hidden inside a picture. This research paper gave a positive side to using the LSB algorithm to implement image steganography and audio steganography. Their results also showed that the amount of data that can be hidden inside the image was increased by 50%. There was also one such paper in which the authors have stated that there are several disadvantages of utilizing LSB that is there will be a reduction in the standard of the stego-image, the authors of this paper also suggested that the method LSB cannot be implemented alone that is it should be combined with some other algorithm that will enhance the secrecy of the data that is being hidden inside the image (Mishra & Bhanodiya, 2015). In the research paper by the authors (Phadte & Dhanaraj, 2017) have implemented a newly modified randomized LSB method in which the

algorithm is used to hide one image inside a different carrier image, the advantage of this research was that, they developed such a model that provided less loss of the quality of the retrieved image at the receiver's side, they also concluded that their method of hiding the data has provided an increased hiding capacity of the stego image. The researcher (Chikouche & Chikouche, 2017) implemented a prototype for hiding a message inside an image file using the LSB algorithm, they also used the Deflate method, which is a lossless data compression technology that integrates the LZ77 and Huffman algorithms to minimize the length of the concealed message. As per (Thangadurai & Devi, 2014), they have constructed picture-established steganography in addition to cryptographic approaches to provide higher security. The researcher of the study has explained the differences between cryptography and steganography, as well as the strength of cryptography and steganography when used together. The researcher has described many techniques for embedding hidden text in a grayscale image using the Least Significant Bit. According to (Khan, et al., 2015) hiding information in the margins can improve the stego image's quality significantly. By swapping the four least significant bits of the cover picture with the secret message, the researcher has employed the spatial domain data hiding approach to hide the secret message in the real edges. Hiding a secret message solely in true edges decreases the concealing capacity slightly but concealing data in true margins pixels minimizes histogram fluctuations to practically nil and histogram modifications, resulting in a high-quality stego image.

3 Research Methodology

The research methodology explains how the planned study will be carried out in detail. This section outlines the step-by-step procedure to secure the data with double protection to achieve confidentiality and secure data transmission. The entire prototype is developed to assure that sensitive data is securely sent from one end toward the other. The target concept of building, this prototype is to improve the already existing prototypes. Cryptography and steganography are combined in the proposed paradigm, with cryptography encrypting the concealed text and steganography concealing the encrypted file. Encryption ensures confidentiality, whereas steganography hides the encrypted text's presence. Below is the step of the developed system, figure 1 represents the block diagram representation of the below-mentioned steps:

Step 1: The first step is to input the personal data in text format. The encryption-decryption AES algorithm is then used to encrypt the secret message; encryption converts the text into meaningless.

Step 2: The outcome of the encryption procedure will be an encrypted text that will be buried inside a picture or an audio file utilizing the steganography concept.

Step 3: Image and audio steganography are both performed using the LSB (Least-Significant-Bit) method. The idea of LSB is such that it will replace the least significant bit of the image or audio with the bit of the data that is being embedded (Singh, et al., 2015).

Step 4: The next step is to retrieve the encrypted text back from the stego-image or stego-audio (depending on the carried medium chosen in the previous step); the extraction process is then performed.

Step 5: After the encrypted text is extracted from the stego-image or stego-audio, the encrypted text is then decrypted using the decryption process of the AES algorithm to get back the original secret text message.

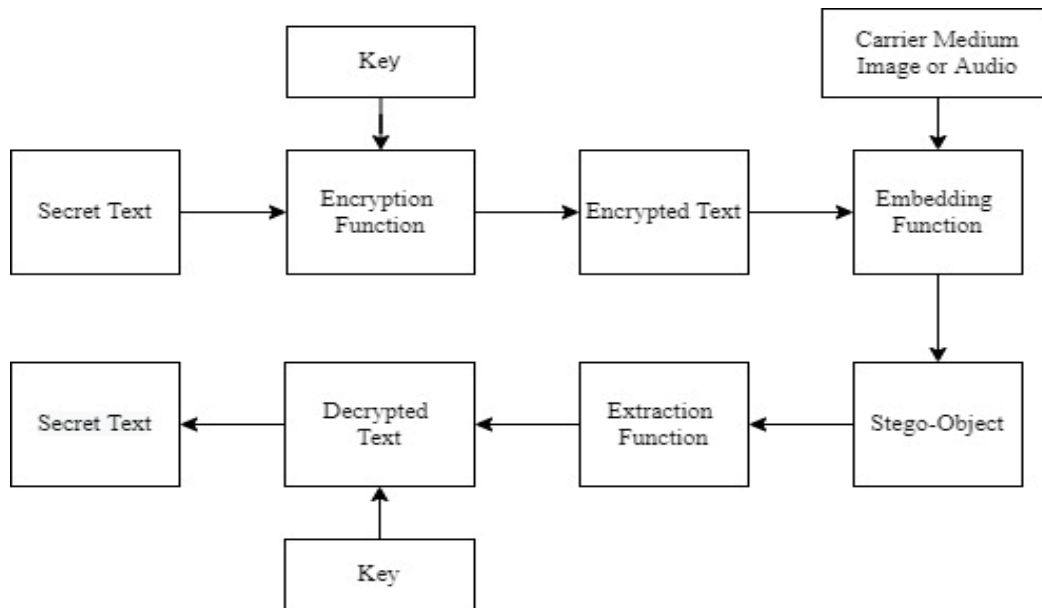


Figure 1: Flow chart of the prototype

The text is encrypted using the Advanced Encryption Standard (AES) method. According to the literature assessment completed in the preceding section, the AES algorithm is one of the finest algorithms for usage in situations where data integrity and secrecy are paramount. After doing a literature review of several cryptographic algorithms, the decision to adopt the Advanced Encryption Standard (AES) algorithm was taken. The Least Significant Bit approach is used to hide data within a picture or an audio file. This algorithm was finalized based on the comparisons of results of different research paper that studies the current available steganographic techniques.

The data used in this prototype are divided into two categories: the carried image used can be any user-owned image (the chosen image should be a .png format only), and the stego image produce should always be saved in .png format only, .jpeg is not considered because it is a compressed form of the image and it will compress the data that has to be embedded and thus the data might be lost. The carrier audio can be either user-owned recorded audio or a public-owned audio file that can be downloaded from any website (the chosen audio should be in .wav format only), the reason for only using .wav file is that as it is an uncompressed raw format the data embedding capacity of the .wav audio file is high as compared to the

capacity of a .mp3 format, which has a low data embedding capacity and also has a higher probability of producing distortion in the quality of the stego-audio.

4 Design Specification

In this section, the architectural views of the system generated by combining the technologies that are covered in the research methodology section are represented and elaborated. To fully comprehend the built system, a step-by-step block diagram was generated, the suggested system's architecture is depicted in the diagrams below; the AES and LSB algorithms are the core components, each of which has its own set of capabilities, it assists us in maintaining the secrecy of the secret data.

Advanced Encryption Standard (AES)

AES is a symmetric method of encryption since it encrypts and decrypts data using the same key (Bernstein & Cobb, 2021). The 128-bit encryption key used by the AES-128 block cipher has ten rounds. This algorithm can be divided into four steps (Mustafeez, n.d.):

Step 1: Subbytes - The bytes of the text block are first replaced according to rules imposed by present S-boxes (short for substitution boxes).

Step 2: ShiftRows - The permutation stage follows next. All byte rows except the first are moved by one in this phase.

Step 3: MixColumns - The Hill cipher is used in the third step to further scramble up the text by mixing the block's columns. Hill cipher is a uniform substitution in which a block of characters is replaced with a word, character, number, or other symbols.

Step 4: Addroundkey - The text is then XORed with the appropriate rounded key in the last step.

The below figure 2 represents a detailed step-by-step flow of the AES algorithm for both encryption and decryption methods.

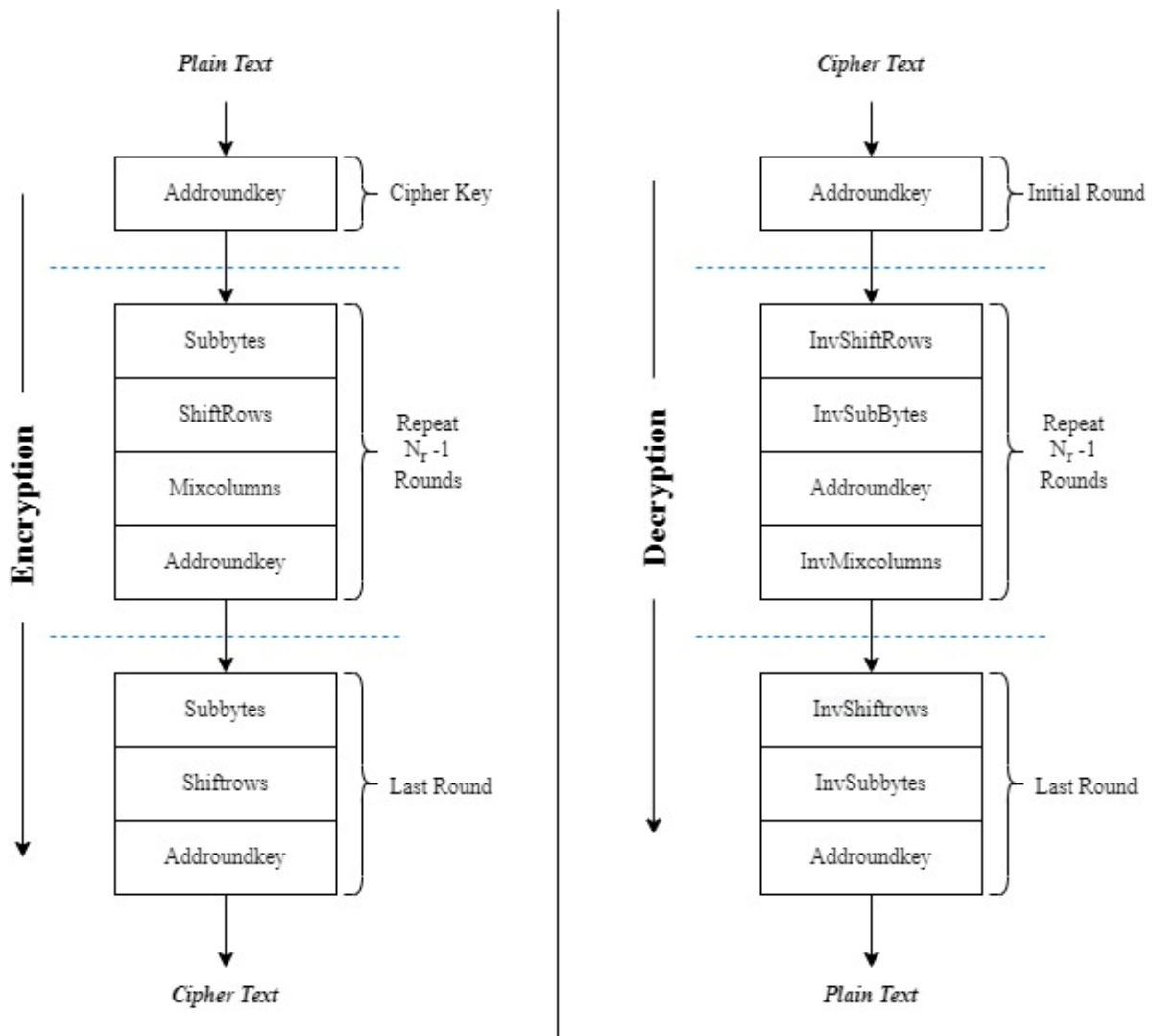


Figure 2: Block Diagram of AES Algorithm (Abood & Guirguis, 2018)

Least Significant Bit (LSB)

Steganography is a technique for concealing confidential information in digital media. Steganography's fundamental goal is to conceal the existence of data in any media, such as image, audio, or video. When it comes to image steganography, the concept is fairly straightforward. Pixels, which generally relate to the colour of that individual pixel, make up images (Sridhar, 2021).

Image Steganography: Image steganography is incredibly reliable and successful, and it may be used for several reasons such as authentication and data concealment. In the least significant bit approach, hidden messages will modify the final bit of a byte in an image (Singh, 2016). The Least Significant Bit is a spatial domain approach in which each bit of information or picture is swapped from the initial image's least significant bit. Since the naked eye cannot discriminate among the original and encrypted image, its presence in the spatial sense is unique (Bandeekar & Suguna, 2018).

Audio Steganography: Audio Steganography is divided into embedding and retrieval. The data is concealed behind a cover medium throughout the embedding process, resulting in stego-audio as result. During the extraction phase, the embedded data is extracted from the stego-audio, which is the reverse of the embedding process (Paniker, et al., 2020). Secret messages are embedded in digitized audio signals in an audio Steganography system, which causes the binary sequence of associated audio files to change. The below figure 3, illustrates the embedding of a message bit in the least significant bit of the audio signal.

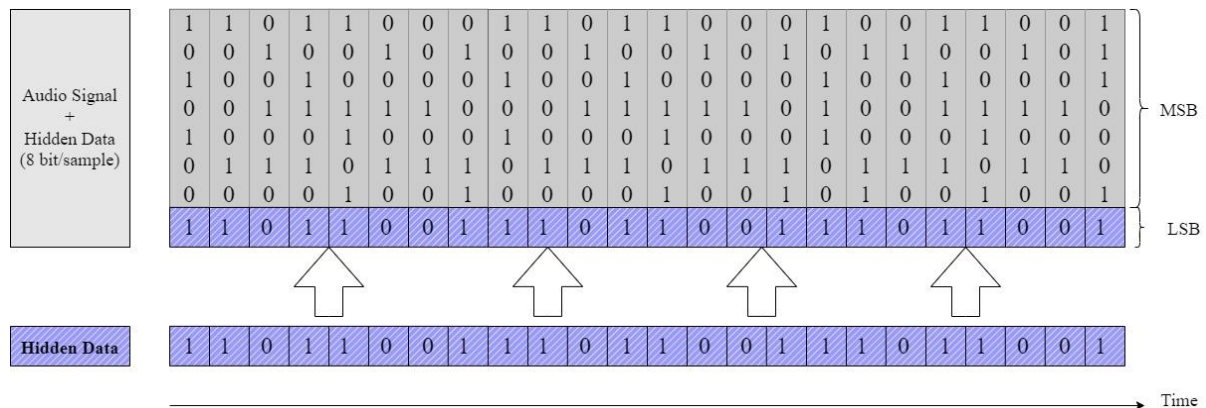


Figure 3: 8bit/ sample with LSB (Djebbar, et al., 2012)

5 Implementation

The suggested method is illustrated in this study by implementing the encryption/ decryption program on a Windows OS using Python 3.8. The.txt file containing the secret information is encrypted and decrypted using the AES-128-bit technique. As the first step of the AES-128-bit algorithm, the user has to input a 16-digit secret key. The 16- character bit has to be entered as 1 character is 8 bits which imply $6 \times 8 = 128$ bits, and as the prototypes use the AES-128-bit algorithm for encrypting the text file it is necessary to enter a 16-character key. Figure 4 illustrates the user has entered a 16 characters key. Figure 4 also illustrates the before and after the quality of the image after encrypting and embedding the .txt file inside that image. After performing the encryption and embedding the system calculates the PSNR and MSE value of the stego-image. To save the stego image the relevant naming has to be given with the extension .png. After the user selects an appropriate stego- image for decryption and de-embedding step, a pop-up notification comes indicating a decoded file has been saved, this is demonstrated in figure 5.

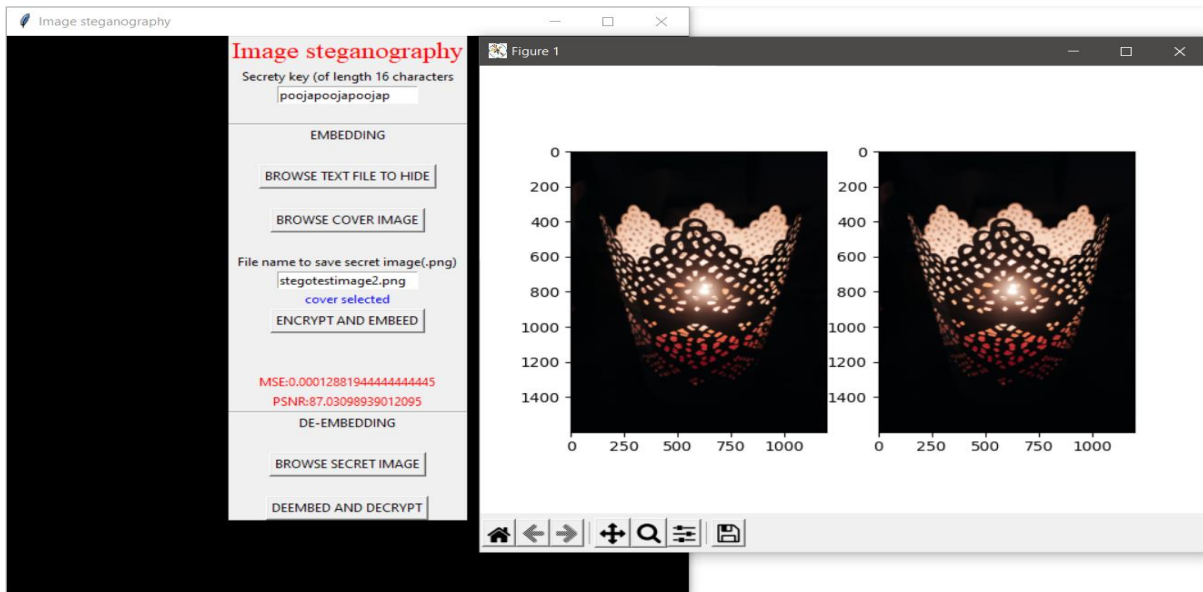


Figure 4: Test Output 1 after embedding the encrypted text inside a carrier image

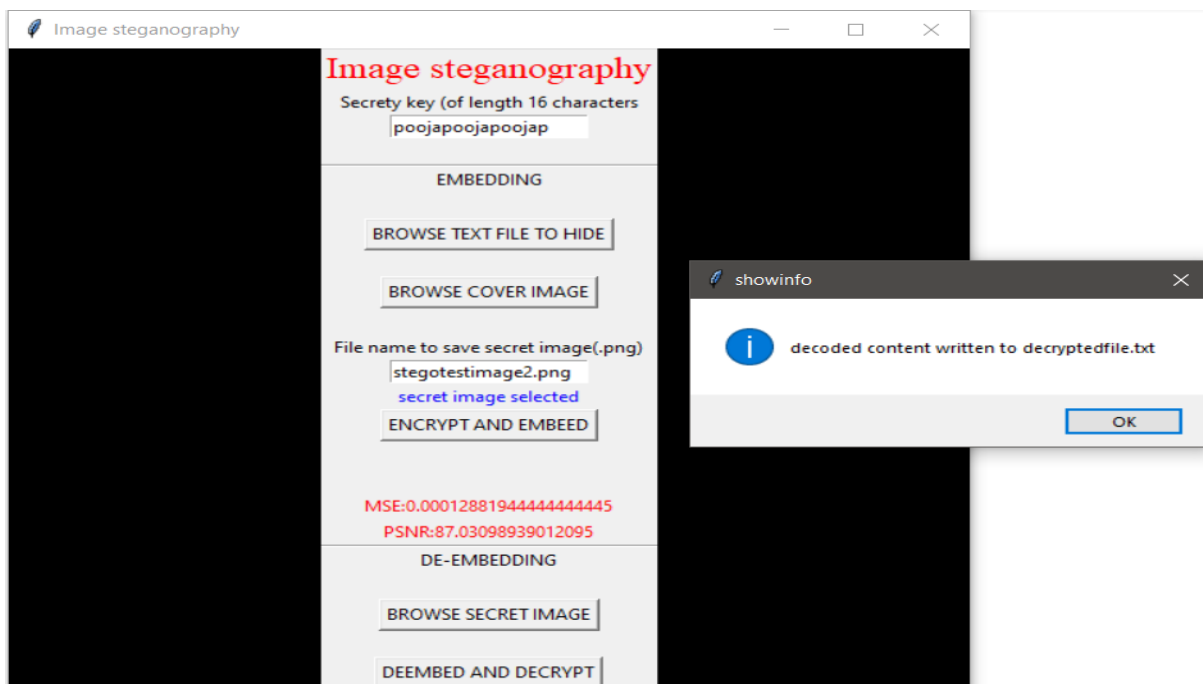


Figure 5: Test Output 1 indicating that the hidden encrypted text file is de-embedded and decrypted in a single step and saved as decryptedfile.txt

The second part of the prototype is the combination of cryptography and steganography, Figure 6 represents after the secret text file is selected it will be encrypted and embedded inside the chosen audio .wav file. Figure 6 also represents the side-by-side comparison of the spectrograph of the original audio and stego audio. After performing the encryption and embedding the system calculates the Peak signal-to-noise ratio (PSNR) and Mean squared error (MSE) value of the stego-audio. To save the stego audio the relevant naming has to be given with the extension .wav. After the user selects an appropriate stego-audio for decryption and

de-embedding step, a pop-up notification comes indicating a decoded file has been saved, this is demonstrated in figure 7.

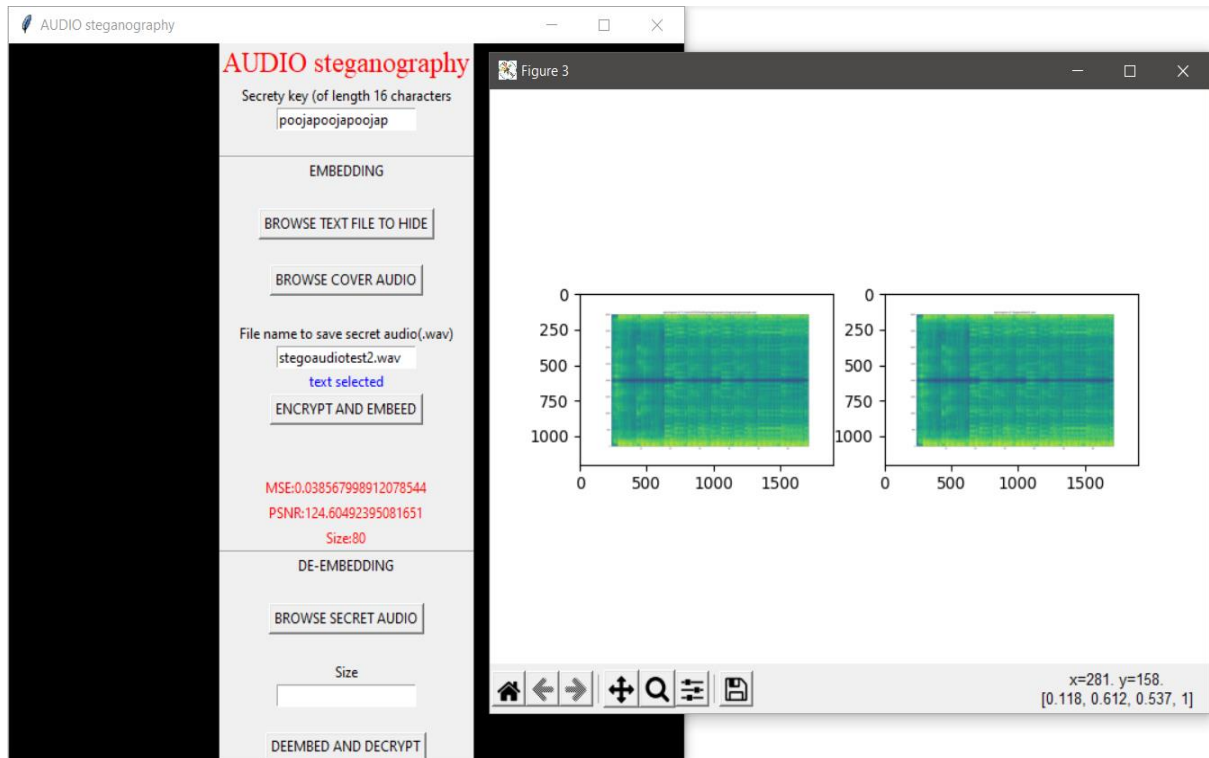


Figure 6: Test Output 1 comparing spectrographs before and after embedding the encrypted text inside a carrier audio

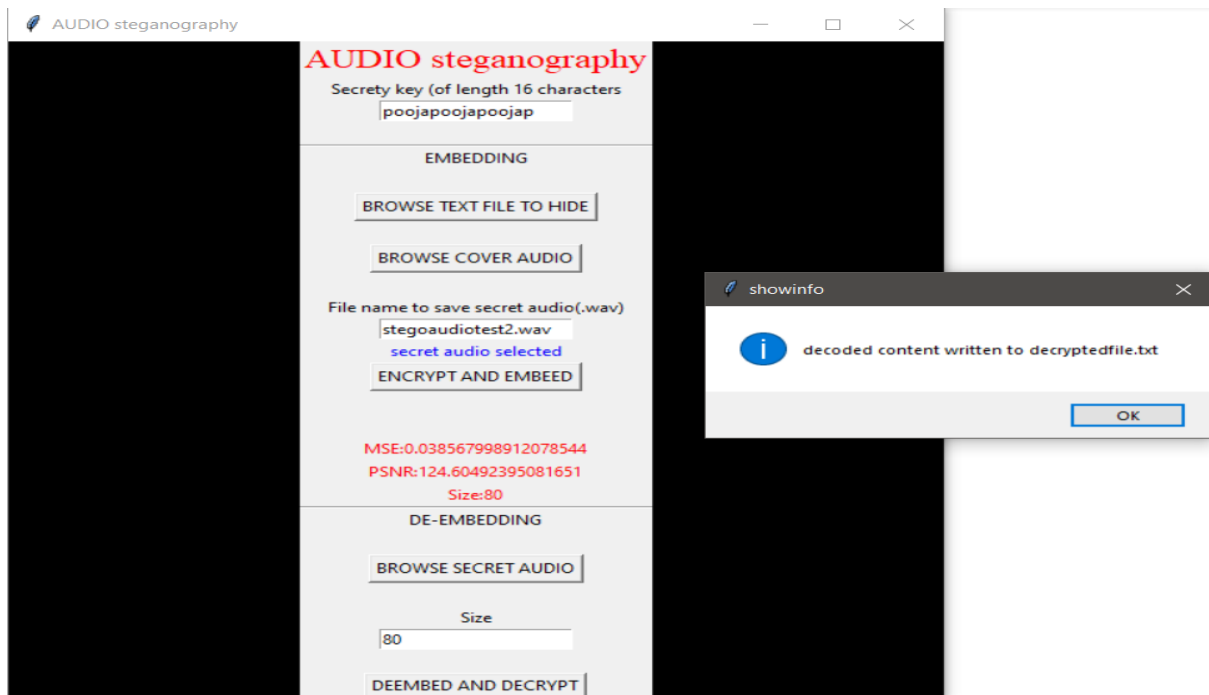


Figure 7: Test Output 1 indicating that the hidden encrypted text file is de-embedded and decrypted in a single step and saved as decryptedfile.txt

5.1 Evaluation metrics

Evaluation metrics: The standard and the quality of the developed system are measured using evaluation metrics. Below mentioned are 4 different types of measures used to evaluate the output generated.

1. MSE

Mean-Square Error (MSE) refers to the image's byte-by-byte calculation and comparing efficiency. When the Mean-Square Error (MSE) reflects a less error rate, the photograph is considered clean (Shetty, 2020). If the MSE value of the output image is zero, then it indicates that there is no presence of noise in the image. It's important to mention that an MSE of 0 indicates complete similarity. A figure greater than 1.0 implies there's less similarity and will continue to rise as the mean-variance amongst pixel intensities increases (Abbas, 2020).

The formula below is used to calculate the MSE value of the modified image:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2$$

In the above equation, m and n represent the width and height of the image respectively.

2. PSNR

The peak signal-to-noise ratio (PSNR) is a popular statistic for evaluating the quality of the image. The Peak Signal-to-Noise Ratio is used to determine the compressed image's quality. The higher the PSNR number, the better the quality of the transformed picture; in other words, the higher the PSNR score, the higher the compression or restoration precision. This measurement tool is used to assess the quality of imperceptibility, particularly in steganography images.

The formula below is used to calculate the PSNR value of the modified image:

$$PSNR = 20 * \log_{10} (max_pixel / \sqrt{(mse)})$$

3. Spectrograph

A spectrogram is a graph that depicts the frequency spectrum of audio files over time. For the evaluation, the spectrograph of the original audio and stego audio are compared side by side.

4. Encoding and Decoding Time

Encoding time is the total time taken by the prototype to encrypt and embed the text file inside an image or audio file. Decoding time is the total time taken by the prototype to decrypt and de-embed the file hidden in the stego image/ audio file.

6 Evaluation

The purpose of the evaluation is to determine the quality of results obtained from the developed prototype. The strength of the proposed prototype, the combination of cryptography with steganography can be determined by calculating the PSNR, and MSE value of the stego image/audio and by plotting the original and stego image and generating a spectrograph of the original audio and stego-audio.

The picture quality characteristics were checked using picture quality measurements such as Mean Square Method (MSE) and Peak Signal to Noise Ratio (PSNR). A higher PSNR value indicates that a picture is of higher quality, while a higher MSE value indicates that the images are not similar. It's worth noting that an MSE value of 0 implies perfect similarity. A number larger than one indicates that there is less resemblance, and it will keep rising as the mean variation amongst the pixel intensity values grows. The MSE is a non-negative metric of an estimator's quality, with values closer to zero being preferable.

6.1 Experiment / Case Study 1

This experiment aims to evaluate the stego image by calculating the PSNR and MSE values respectively as suggested above a higher PSNR value indicates the resulting image is of higher standards and an MSE value of 0 indicates there is almost no variation between the original image and the stego image.

The Peak signal-to-noise ratio and Mean squared error values obtained for both the test cases, as depicted in Table 1, illustrate that the stego image produced is of high quality and has a negatable difference compared to the original image. Thus, from the below results it can be proved that the prototype produces a high-quality standard stego image which will be unnoticed by the attacker as there is no dissimilarity in the original and stego image.





Index	Original Image	Stego Image	PSNR	MSE
1			87.0309	0.000128
2			87.1858	0.000124

Table 1: Experimental cases for Image Steganography

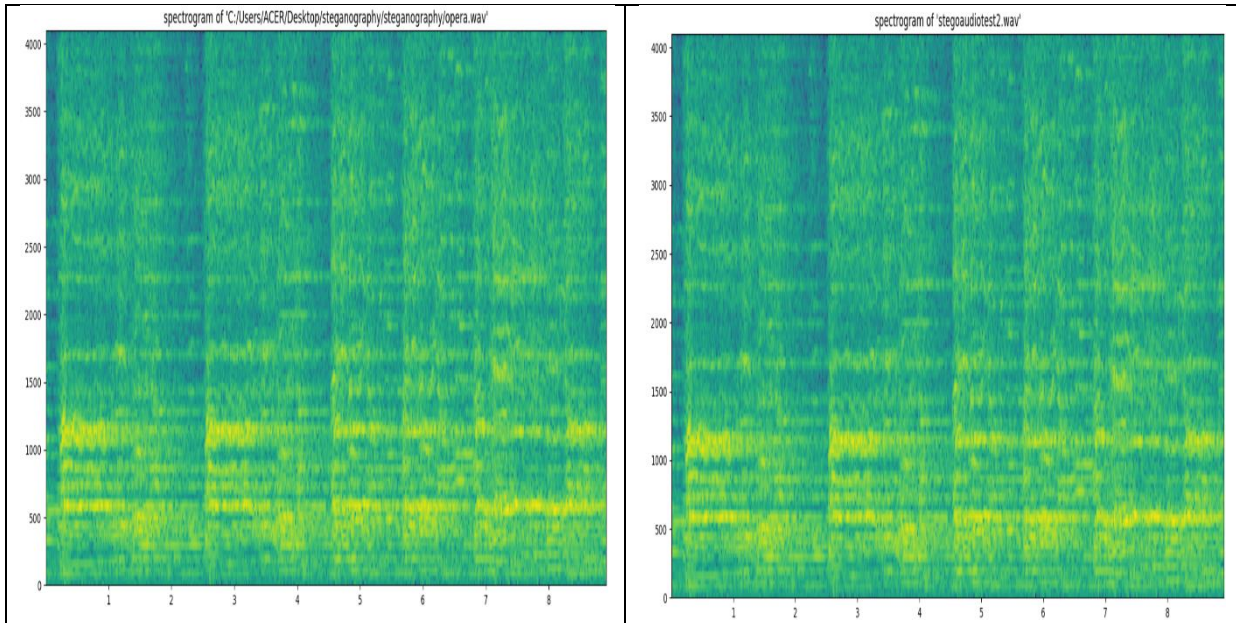
6.2 Experiment / Case Study 2

This experiment aims to evaluate the stego audio by calculating the PSNR and MSE values respectively and representing the audio waves in the form of the spectrograph for both stego audio, as suggested above a higher PSNR value indicates the resulting audio is of higher standards and an MSE value 0 indicates there is almost no variation between the original audio and the stego audio.

The Peak signal-to-noise ratio and Mean squared error values obtained for both the test cases, as depicted in Table 2 illustrate that the stego audio produced is of high quality and has a negatable difference compared to the original audio. Thus, the below results prove that the prototype produces a high-quality standard stego audio which will be unnoticed by the attacker as there is no dissimilarity between the original and stego audio.

6.1 Experiment / Case Study 2

Result Analysis for audio: Opera.wav	
Original Audio Spectrograph	Stego-audio Spectrograph



MSE of stego audio: 0.07350235357839086

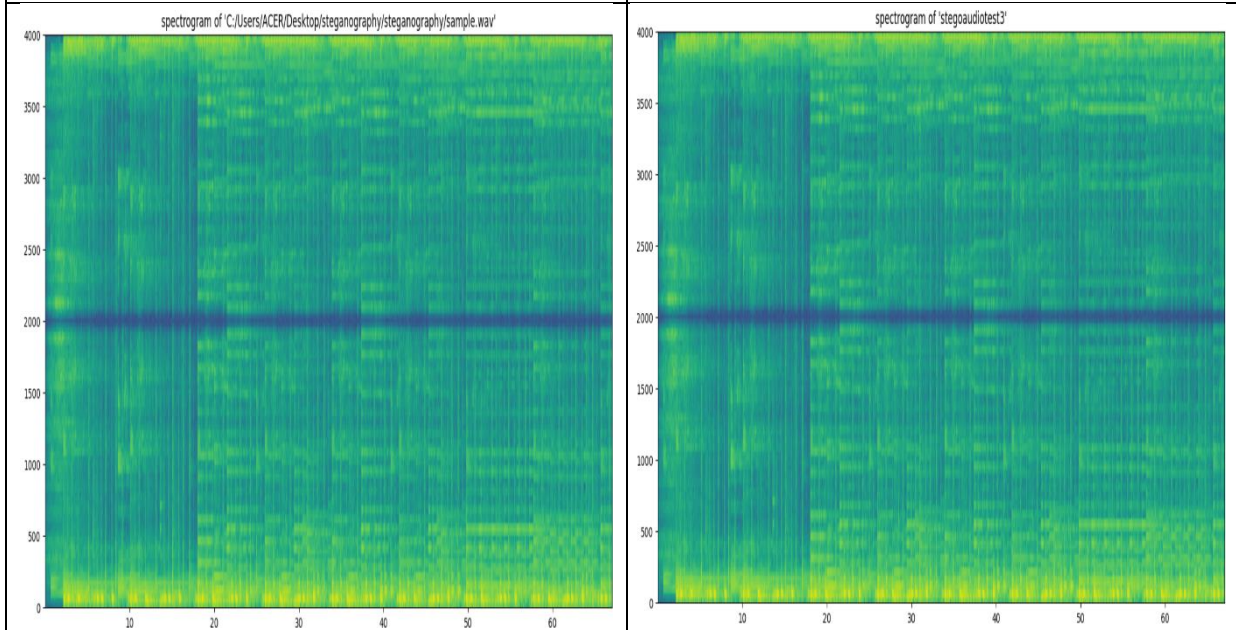
PSNR of stego audio: 119.0034411630788

Table 2: Experimental Case 1 for Audio Steganography

Result Analysis for audio: Sample.wav

Original Audio Spectrograph

Stego-audio Spectrograph



MSE of stego audio: 0.038567998912078544

PSNR of stego audio: 124.60492395081651

Table 3: Experimental Case 2 for Audio Steganography

6.2 Discussion

The following table is summarized after performing the above experiments. The table below summarizes experimental examples for various text measurements, as well as the PSNR, MSE, encoding, and decoding times.

Text Size (Kb)	Carrier Medium	PSNR	MSE	Encoding Time (secs)	Decoding Time (secs)
176	Test Image 1	87.0309	0.0001	0.2	0.6
176	Test Image 2	87.1858	0.0001	0.4	0.4
80	Test Audio 1	119.0034	0.0735	0.5	0.8
80	Test Audio 2	124.6049	0.0385	0.6	0.5

Table 4: Test Cases

The results obtained in this research work after performing appropriate experiments, it can be concluded that the calculated metrics PSNR and MSE values give a high-quality stego image and also produces a less dissimilar stego image with very few alterations.

The measurements for the above table are as followed: the size of the text file is in Kb, the encoding and decoding time are the total time for encrypting plus embedding and decrypting plus de-embedding of the text file respectively, these timings are measured in seconds and are manually calculated.

7 Conclusion and Future Work

The prototype works successfully, demonstrated a strategy for encrypting basic text using the AES algorithm and concealing the ciphertext produced using the LSB algorithm in a cover image or audio file. There are several steganography and cryptography schemes that have been developed, each with its own set of benefits and drawbacks. The suggested approach produces high-quality steganography, with no discernible differences in the carrier file following steganography. The suggested approach conceals the encrypted message inside the carrier image or audio file with few alterations and without affecting the integrity, as evidenced by spectrograms, Peak signal-to-noise ratio (PSNR) and Mean squared error (MSE) values. If the assaulter succeeds in breaking the steganography, they will be given an encrypted message since the original message would be encrypted first when the steganography is performed. At the sender's side, the text is encrypted and concealed in a carrier image or audio; at the recipient's side, it is decoded and decrypted. With minimum alteration, this method is effectively shown in this study. The suggested solution effectively maintains the secrecy of the given text form. Primarily text is being encrypted and concealed in a cover image or audio track in the current system; but, in the near term, additional file types could be encrypted and concealed utilizing a similar approach. Various video file types could be used as the cover object to effectively disguise the encrypted message/information/ information. To guarantee secrecy to the input information, several groupings of cryptography and steganography methods might be tested.

8 References

- Abbas, F. H., 2020. Securing secret data using an enhanced, Dublin, Ireland: s.n.
- Abood, O. G. & Guirguis, S., 2018. A Survey on Cryptography Algorithms. International Journal of Scientific and Research Publications, July, 8(7), pp. 495-516.
- Alam, S., Zakariya, S. & Rafiq, M., 2013. Analysis of Modified LSB Approaches of Hiding Information in Digital Images. Mathura, India, IEEE, pp. 27-29.
- Bandekar, P. P. & Suguna, G. C., 2018. LSB Based Text and Image Steganography Using AES Algorithm. Coimbatore, India, s.n.
- Bernstein, C. & Cobb, M., 2021. Advanced Encryption Standard (AES). [Online] Available at: <https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard> [Accessed 11 11 2021].
- Bindra, S. D. & Bawa, N., 2018. AES Hybridization with Genetic Technique for guarded Image Transmission. Coimbatore, India, IEEE, pp. 20-21.
- Chikouche, S. L. & Chikouche, N., 2017. An improved approach for lsb-based image steganography using AES algorithm. s.l., IEEE, pp. 1-6.
- Djebbar, F., Ayad, B., Meraim, K. A. & Hamam, H., 2012. Comparative study of digital audio steganography techniques. EURASIP Journal on Audio, Speech, and Music Processing, 9 October.
- Gautam, A. C., 2019. Secure End to End transmission using, Dublin: s.n.
- Khan, S. et al., 2015. A secure true edge based 4 least significant bits steganography. Peshawar, Pakistan, 2015 International Conference on Emerging Technologies (ICET).
- Mishra, R. & Bhanodiya, P., 2015. A review on steganography and cryptography. s.l., 2015 International Conference on Advances in Computer Engineering and Applications, pp. 119-122.
- Mustafeez, A. Z., n.d. What is the AES algorithm?. [Online] Available at: <https://www.educative.io/edpresso/what-is-the-aes-algorithm> [Accessed 4 11 2021].
- Paniker, P., Dahare, V. & Saurkar, A., 2020. Data Hiding using Cryptography and Image/Audio Steganography. International Research Journal of Engineering and Technology (IRJET), May, 07(05), pp. 1565-1571.
- Phadte, R. S. & Dhanaraj, R., 2017. Enhanced blend of image steganography and cryptography. Erode, India, 2017 International Conference on Computing Methodologies and Communication (ICCMC), pp. 230-235.
- Raphael, A. J. & Sundaram, D. V., n.d. Cryptography and Steganography – A Survey. International Journal of Computer Technology and Application, Volume 2 (3), pp. 626-630.

Semwal, P. & Sharma, M. K., 2017. Comparative study of different cryptographic algorithms for data security in cloud computing. Dehradun, India, 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall), pp. 1-7.

Sheth, U. & Saxena, S., 2016. Image steganography using AES encryption and least significant nibble. Melmaruvathur, India, 2016 International Conference on Communication and Signal Processing (ICCSP), pp. 0876-0879.

Shetty, A., 2020. Securing Confidential Data using Dual, Dublin, Ireland: s.n.

Singh, A. K., Singh, J. & Singh, D. H. V., 2015. Steganography in Images Using LSB Technique. International Journal of Latest Trends in Engineering and Technology (IJLTET), January, 05(01), pp. 426-430.

Singh, P., 2016. A Comparative Study of Audio Steganography Techniques. International Research Journal of Engineering and Technology (IRJET), April, 03(04), pp. 580-585.

Sousi, A.-L., Yehya, D. & Joudi, M., 2020. AES Encryption: Study & Evaluation. [Online] Available at:

https://www.researchgate.net/publication/346446212_AES_Encryption_Study_Evaluation/citation/download [Accessed 20 10 2021].

Sridhar, A., 2021. LSB based Image steganography using MATLAB. [Online]

Available at: <https://www.geeksforgeeks.org/lsb-based-image-steganography-using-matlab/> [Accessed 08 11 2021].

Thangadurai, K. & Devi, G. S., 2014. An analysis of LSB based image steganography techniques. Coimbatore, India, IEEE, pp. 1-4.