# Image Steganography For Transmitting Confidential Messages

**Afra Fathima M A[1, a)] Gunashri S[2, b)] Janani A[3, c)] Kavyaa A K[4, d)] Jackulin C[5, e)]**

[1,2,3,4] B. E Department of Computer Science and Engineering, Panimalar Engineering College, Tamil Nadu, India

[5]Assistant Professor, Panimalar Engineering College, Tamil Nadu, India

**Abstract.** The art of concealing data such as text, images, or videos, inside a cover image is known as image steganography. Steganography is carried out using a variety of concepts, including traditional methods, CNN-based approaches, and GAN-based techniques. [1] It thoroughly describes the soul idea of image steganography approaches of embedding text data in images. This paper seeks to offer quick and effective techniques for performing image steganography, demonstrates their precise and elaborative implementation and its applications.[4] This paper explores about how image steganography can progress in the future by being incorporated into the messaging services we use every day.

*Keywords*-- Steganography, Traditional image steganography techniques, CNN (Convolutional Neural Network)-based image steganography techniques, and GAN (Generative adversarial networks)-based image steganography techniques. LSB (Least Significant Bits).

## INTRODUCTION

The idea of steganography is to hide information inside multimedia. The secret information is concealed so that human eyes cannot see it. This information can be a plain text, image, video or audio that will be embedded into another larger media. Nowadays we have numerous methods for data transmission, but the foremost defect is the insecurity of data.[1]. It is vital to protect the integrity of data while transmitting sensitive military information and significant files in companies [2]. Steganography is divided into 2 words where 'Stegano' – refers to Covered and 'Graphy' – refers to writing in Greek. Steganography is an art of 'Covered Writing'[4].

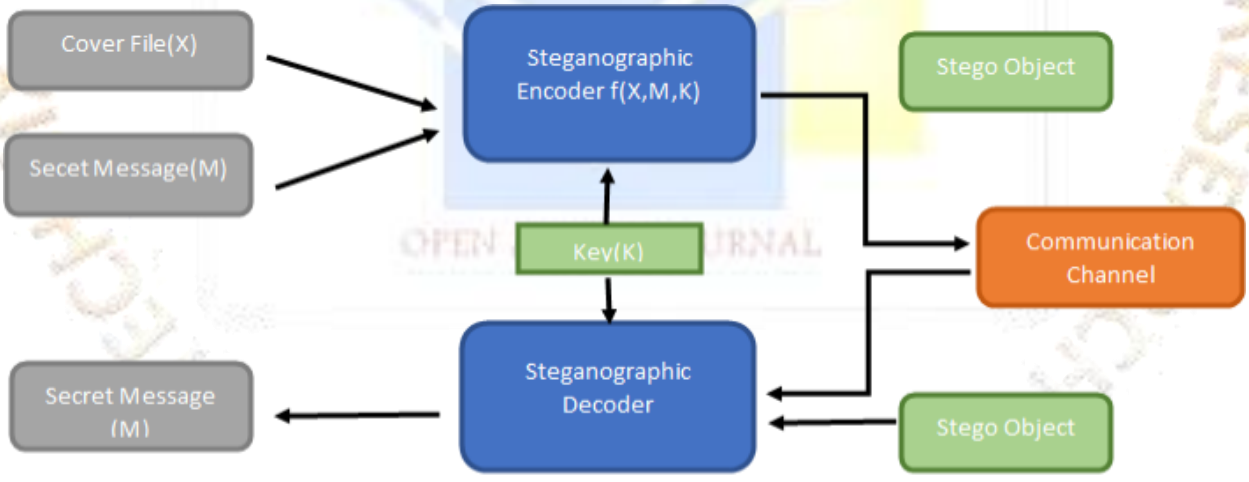


**FIGURE 1**: Steganography architecture

Cryptography and Steganography are both techniques used to shield or safeguard confidential data. However, they differ from one another - cryptography obscures the meaning of the data. Whereas steganography conceals the existence of the data [5].

## Types of Steganography:

Steganography is classified into 5 types:

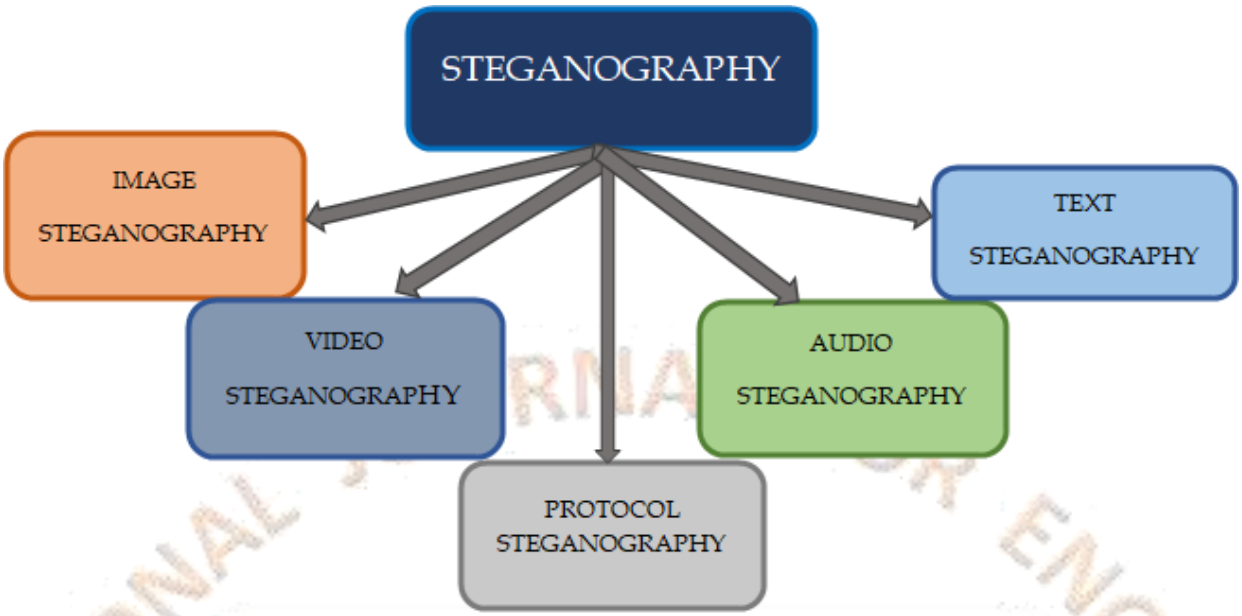


**FIGURE 2**. Types of steganography

1. *Text Steganography:*

Each word's character contains a code that conceals some information.

2. *Image Steganography:*

It involves hiding data by using a cover image of a distinct object. The key to data steganography in images is pixel levels.

3.*Audio Steganography***:**

Unauthorized access can be prevented by embedding information in audio.

4.*Video Steganography*:

It uses discrete transform cosine to insert values to a collection of still images, i.e videos which is invisible to the human naked eye.

5.*Protocol Steganography***:**

It is also known as Network Steganography. It entails encrypting data using a network protocol as a cover object, such as TCP, UDP, ICMP, IP, etc. [6]

## Image Steganography:

The art of image steganography involves concealing data—text, images, or even videos—within a cover picture. The text and image are combined on the sender side to produce a steganographic image. The concealed text is extracted and made visible from this steganographic image on the receiver side.

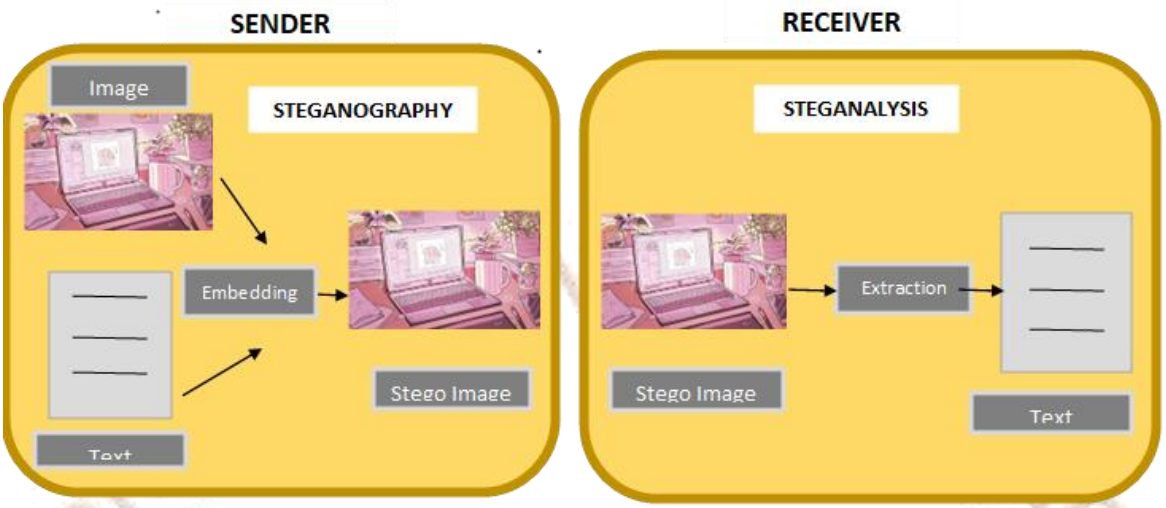


**FIGURE 3**. Image steganography process in sender and receiver side.

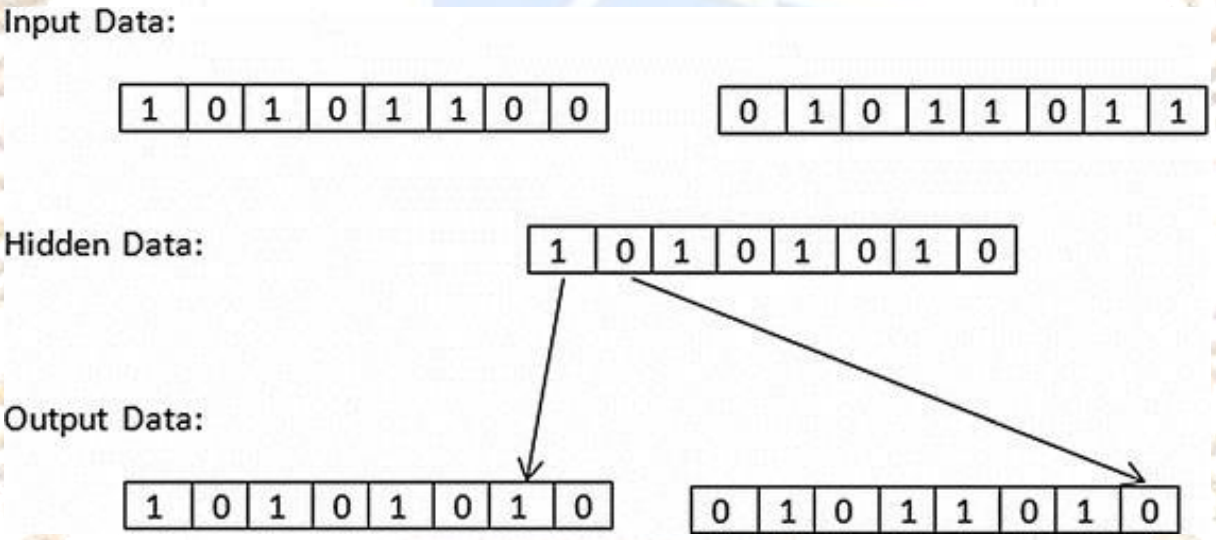


**FIGURE 4.** Least significant bit substitution

## LITERATURE SURVEY

Subramanian, Nandhini, et al [1] have classified image steganography into three types: Traditional image steganography techniques, CNN-based image steganography techniques, and GAN-based image steganography techniques. Deep learning or machine learning are not used in Traditional image steganography. CNN is a machine learning model based on neural networks that extract messages, whereas GAN-based steganography approaches use GAN variations.

### Traditional image steganography:

To steganograph images, the Least Significant Bits (LSB) substitution technique is used. The LSB technique operates under the presumption that changing a small number of pixel values would not result in any discernible changes. The binary-coded secret data is transformed and encoded in the pixel values [9][10]. A discrete wavelet transformation (DWT) and discrete cosine transformation (DCT) combination is used to conceal the secret information within a cover video. The multiple object tracking (MOT) technique is used to locate the regions of interest. Prior to embedding the confidential data in the cover video, it is first encoded and then converted to binary bits[11]. The Pixel Value Differencing (PVD) technique is another traditional method used in the area of image steganography . In order to find the best places to bury the secret bits while still maintaining the consistency of the cover picture, PVD compares the differences between adjacent pixels[12].

### CNN Based Image Steganography:

The evolution of CNN models from the encoder-decoder architecture has had a significant impact on image steganography. To construct the stego image, the encoder needs both the cover image and the secret image as input. The decoder then utilizes the stego image as input to receive the embedded secret image. Here cover image and secret image should be the same size, so that the cover image uses each pixel of the secret image [1].

There are several different architectures that are employed, including Encoder decoder, U-Net, CNN, encoder decoder with VGG basis, and encoder decoder with SCR. Encoder decoder, U-Net, and CNN uses basic design and architecture to hide an image as a hidden message. On the other hand, input photos are concatenated, and the image size is a very modest 64x64 [13][14][15]. Domain expertise is not necessary for encoder-decoder with VGG base. As the created image is unrelated to any personal information, it is quite secure. But adding more photos increases computation. Encoder- Decoder using SCR is extremely reliable and safe. Yet, areas that are black or white can exhibit visual noise [17][18][16].

### GAN Image Steganography:

Deep CNNs are a subset of general adversarial networks. In order to train a generative model with an adversarial process for image creation problems, a GAN leverages game theory. With the GAN architecture, a perfect image is produced through competition between the generator and discriminator networks[19]. GAN is renowned for its excellence in the realm of picture generation[1].

The GAN architectures include Cycle GAN, DCGAN, WGAN, ACGAN, Alice, Bob and Eve, Info-GAN, DCGAN, and ASDL GAN with a variety of datasets[1].

## METHODOLOGY

### Implementation of image steganography using 7-zip:

**STEP 1:** create a folder and name it as “Test”

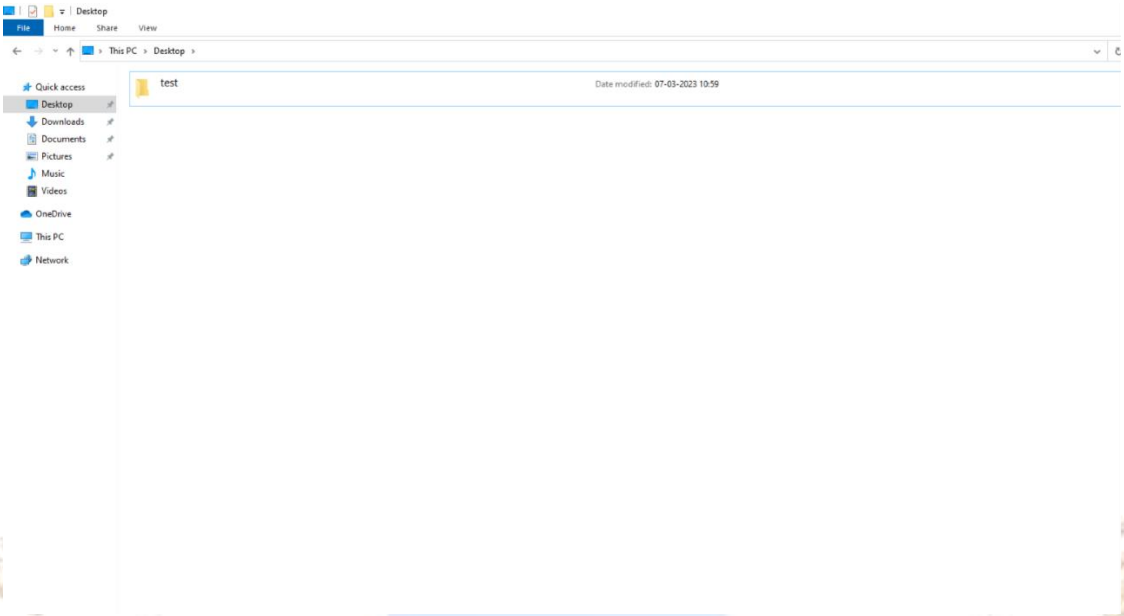


**FIGURE 4**. Creating folder Test

**STEP 2:** Insert an image file into the "Test" folder**.**

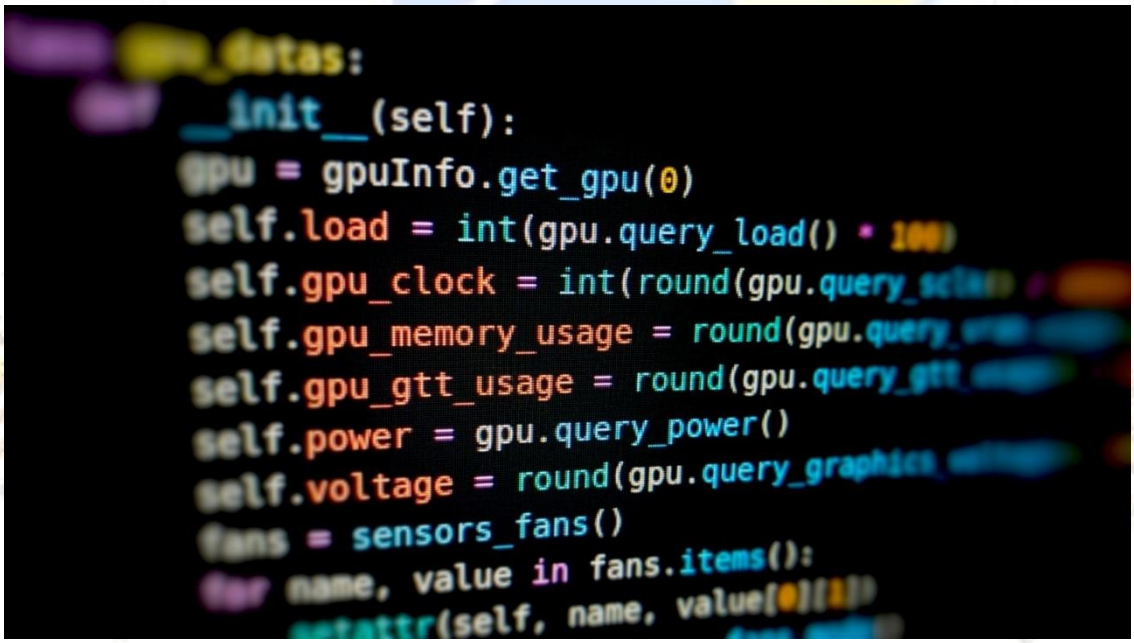


**FIGURE 5**. The image that is added in ‘Test’ folder

**STEP 3:** Create a text document with confidential information in the folder "TEST".

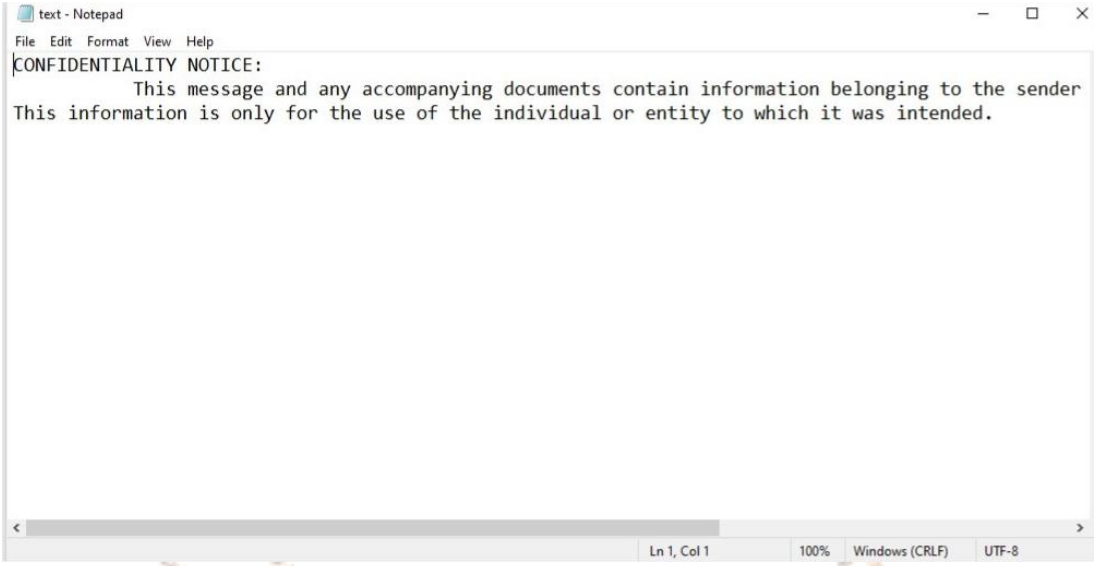


**FIGURE 6.** The confidential information is written in the text document

**STEP 4:** Right click on the image and hover to 7-Zip. Then select "Add to text.zip." This will create a zip folder.

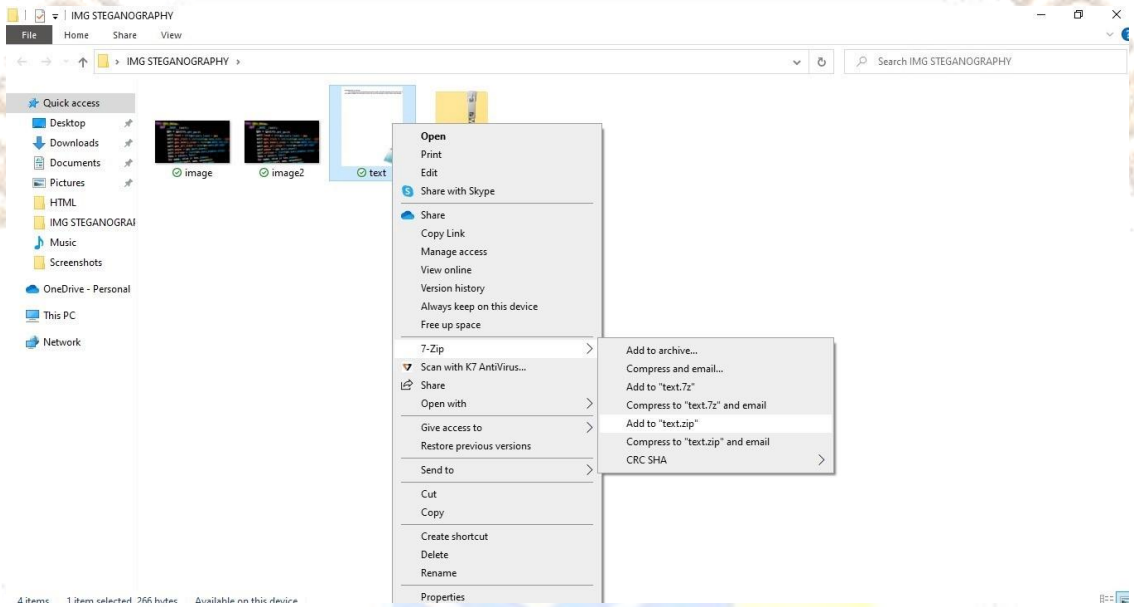


**FIGURE 7.** Creating a zip folder

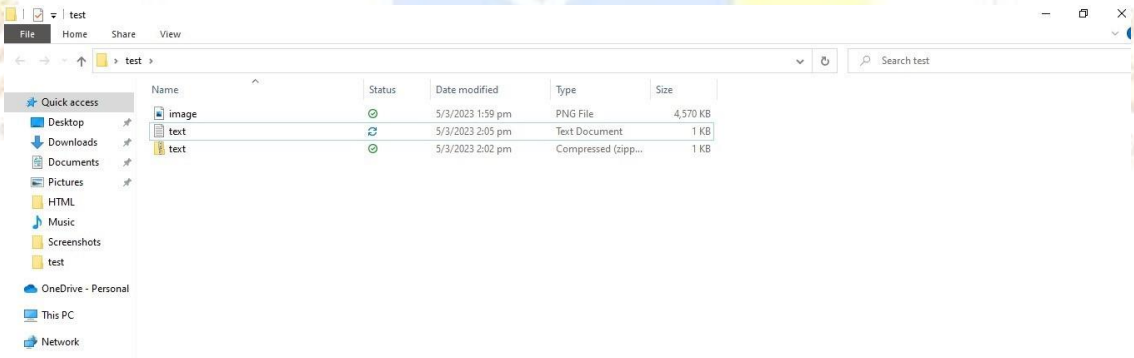


**FIGURE 8**. zip folder is created

**STEP 5:** Open the command prompt and then type:

- cd [folder address] (to access the working folder)
- dir (to pull up a directory of items that are in the folder with the image file.)
- Copy /b image.png+text.zip image2.png (to create an image2.png by combining text.zip with an image.png.)

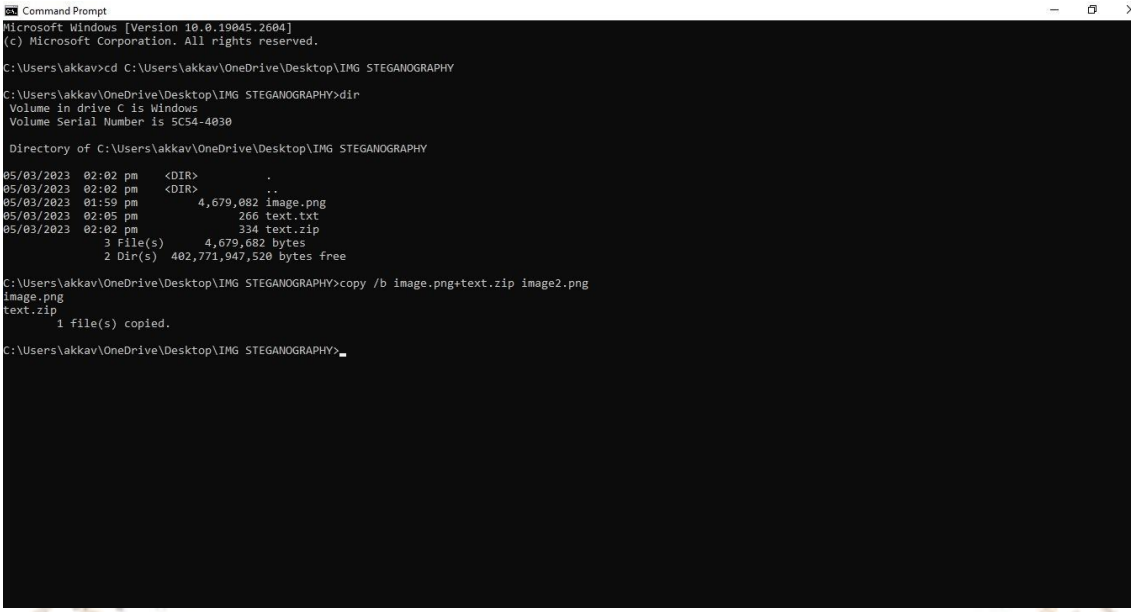


**FIGURE 9**. Embedding

**STEP 6:** Return to the "TEST" folder and there will be a second image in the folder.

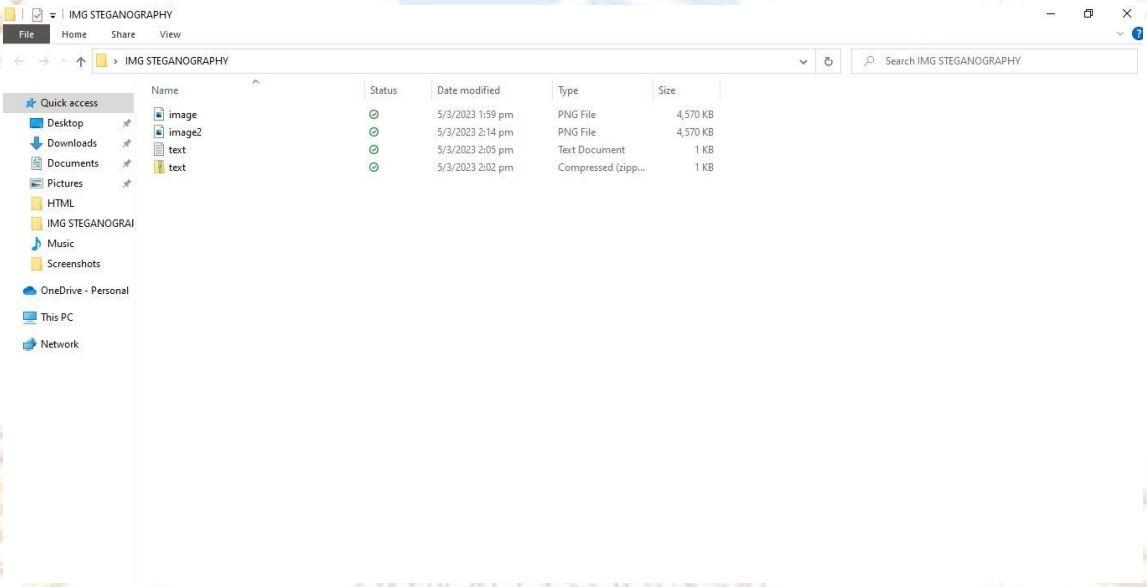


**FIGURE 10.** Appearance of steganographed image.

**STEP 7:** If you open the image 2 file, it will open and appear just like the previous image.

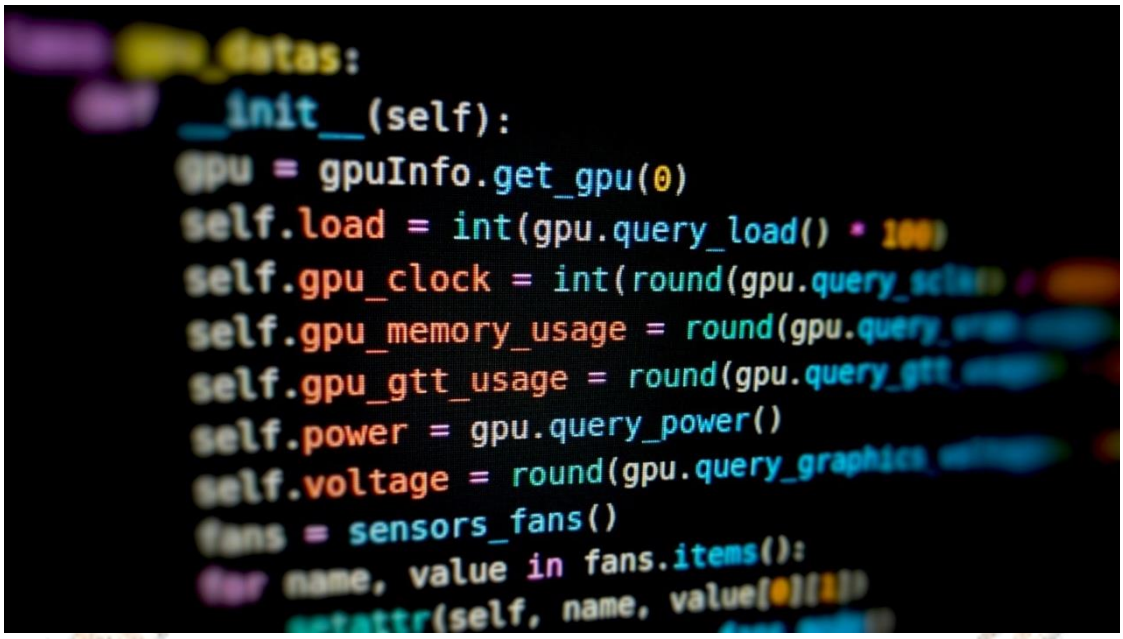


**FIGURE 11**. Image after embedding text into it.

**STEP 8**: open the image2 using 7-Zip, we will be able to see the text file which contains the confidential information.

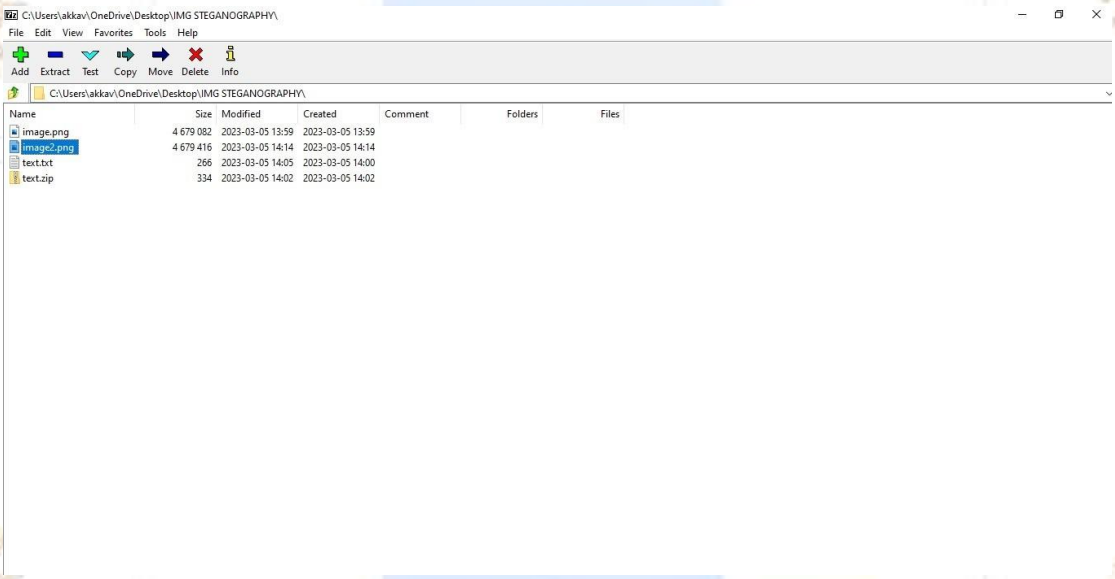


**FIGURE 12.** Extracting text from image using 7-Zip

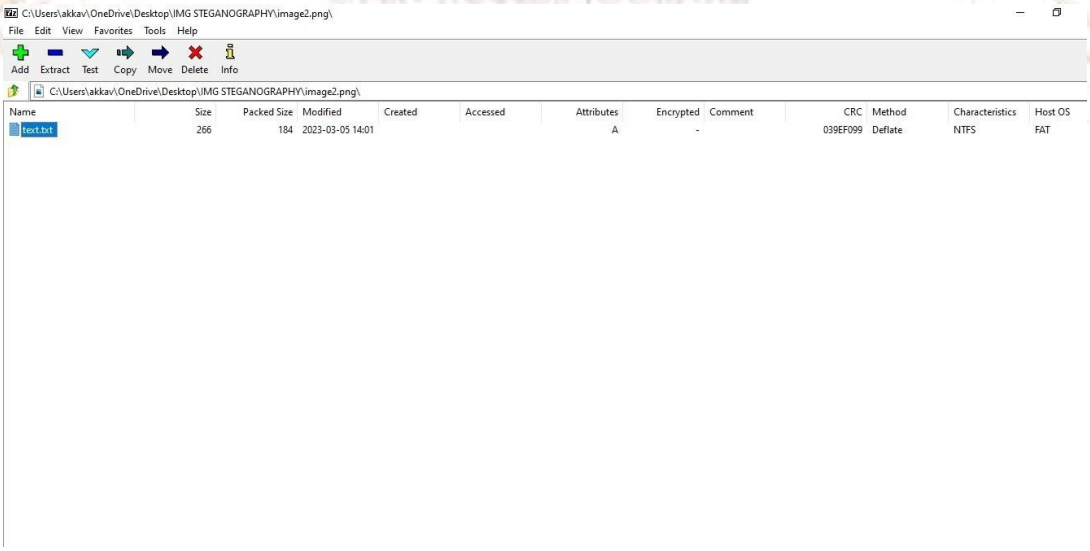


**FIGURE 13**. Text file after extraction.

**STEP 9:** Confidential information can be viewed.

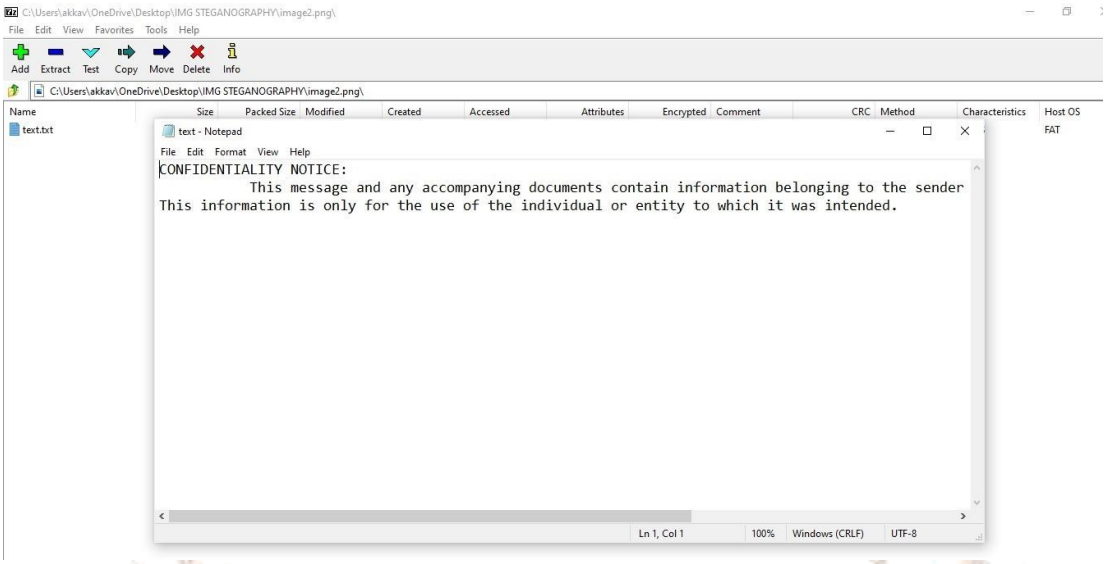


**FIGURE 14**. Confidential text.

**Implementation of image steganography using python:**

Here, we've used Python to create image steganography along with a user-friendly GUI by importing different modules. The system carries out the two tasks of encoding and decoding image data.

**Encoding:**

**STEP 1**: choose the option encode

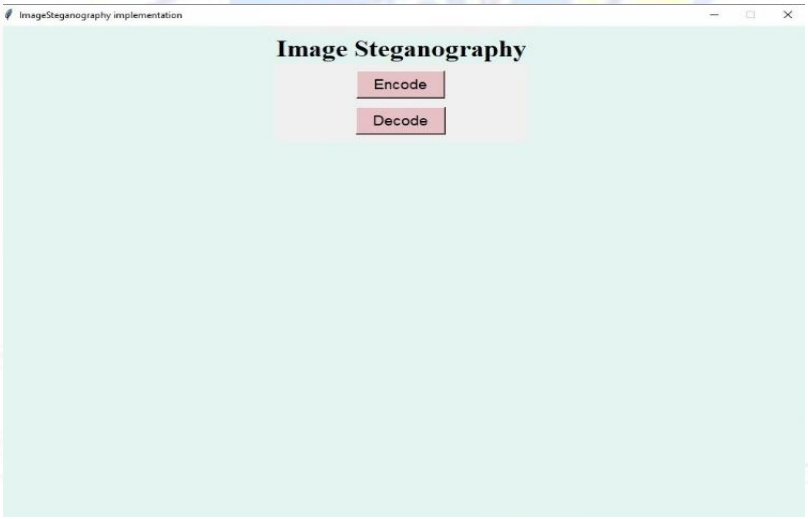


**FIGURE 15**. Application home page with options encode and decode.

**STEP 2**: Select the image for encryption

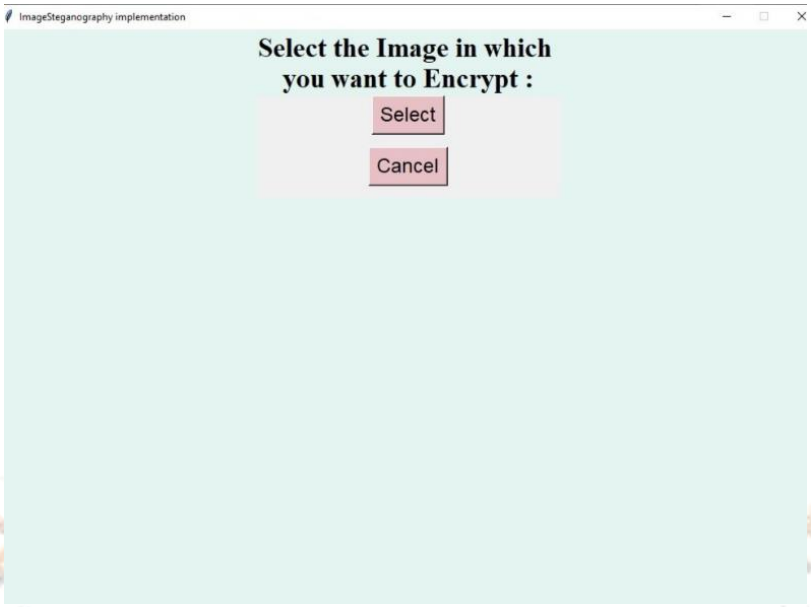


**FIGURE 16.** Selecting image for encryption.

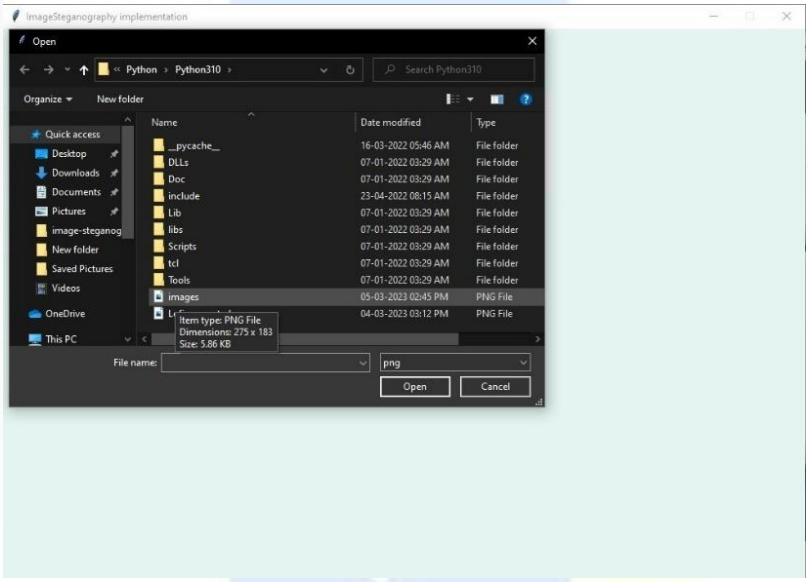


**FIGURE 17.** Choose the image to be encoded

**STEP 3:** message to be encoded

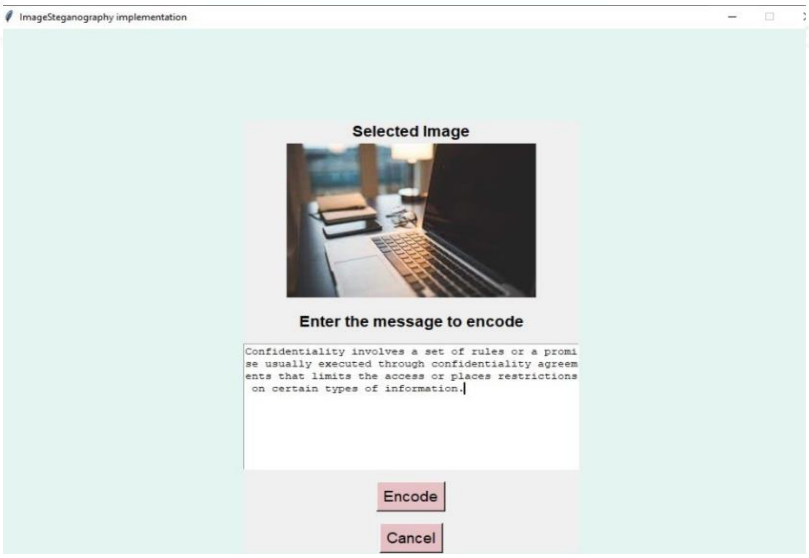


**FIGURE 18.**Information to be encoded

**STEP 4**:Enter the file name

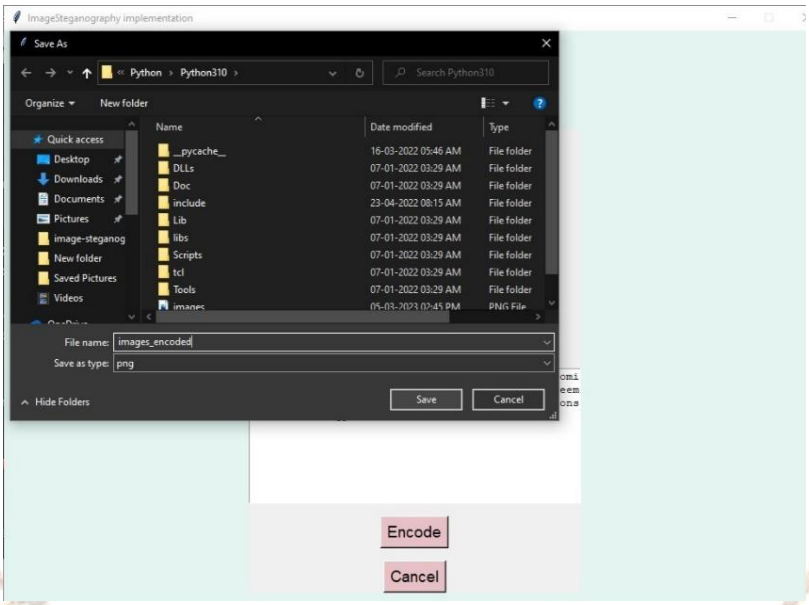


**FIGURE 19**.Saving encoded image

**STEP 5**: ENCODING SUCCESSFUL!!..

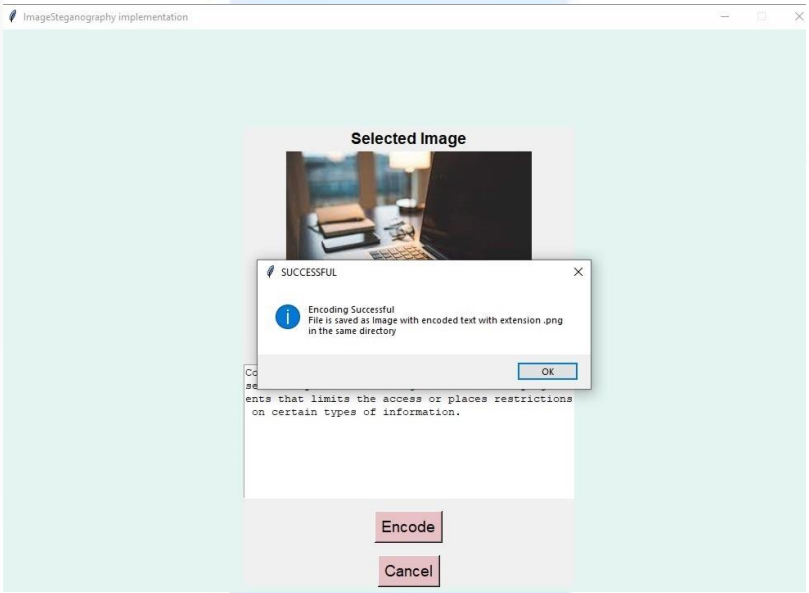


**FIGURE 20**.Encoding completed

**Decoding:**

**STEP 1:** select the image to be decrypted

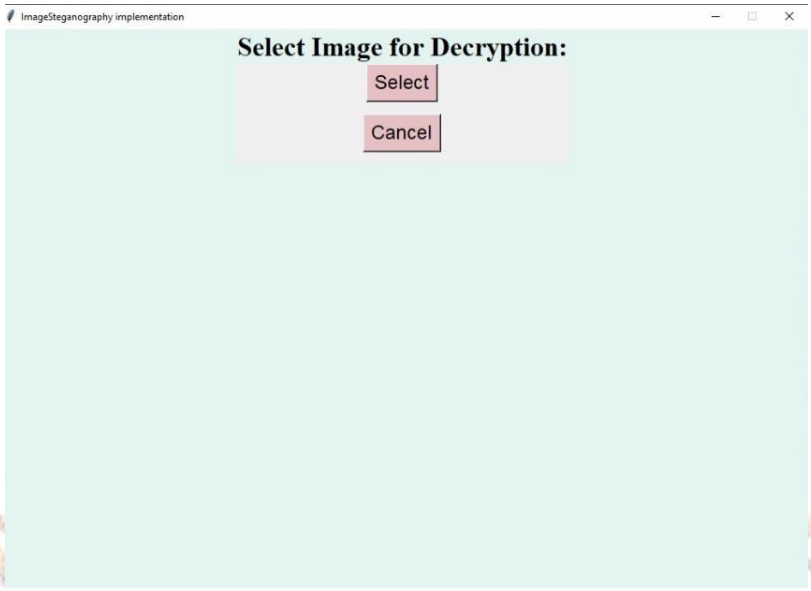


**FIGURE 21**.Decode

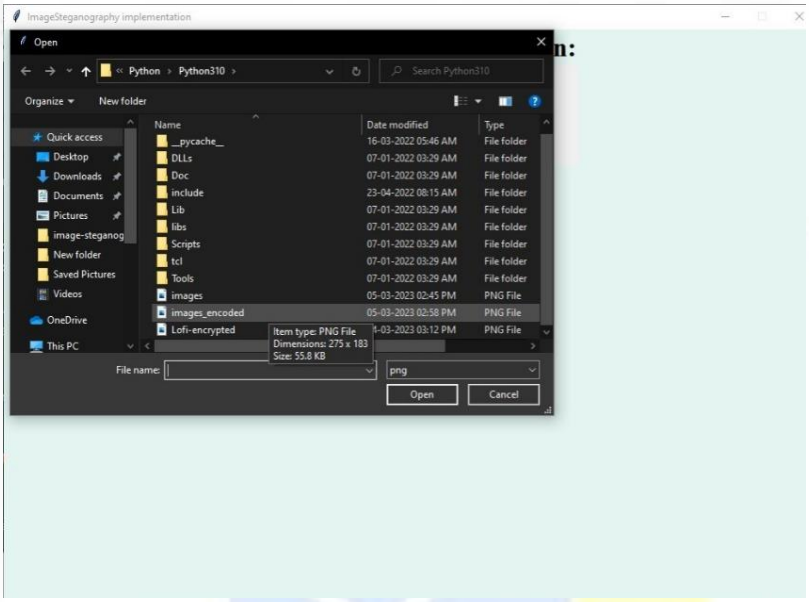


**FIGURE 22**.Choose encoded image

**STEP 2**: DECODING SUCCESSFUL!!...

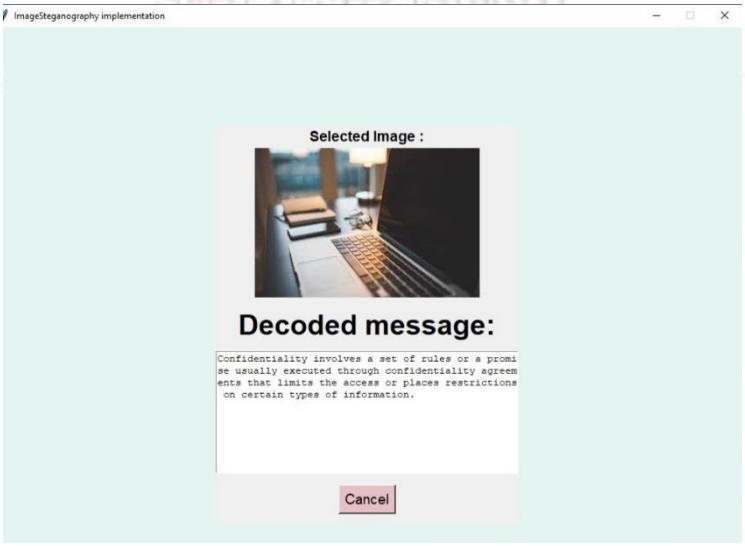


**FIGURE 20**.Decoded message displayed

## APPLICATIONS

The main function of image steganography is to conceal data inside of images, including text, images, and speech. Thus, its main areas of application are those that need the sharing of sensitive information. Every day around the world, businesses and organizations deal with the issue of data leakage [20]. Data loss is more likely as information technology advances. It is better to tighten control over channels while using electronic media and exchanging information since any interference with corporate systems runs the danger of hurting the business. Trade secrets, creations, innovations, databases, and business details must be transferred in a way that the confidential content must be well hidden. The information leak can cause direct financial loss, a decline in company's reputation, and the loss of clients, and confidential data [21]. Hence, steganography is essential for delivering or receiving data with hidden information without alerting a third party to the message's presence. The principal applications of steganography include digital watermarking, network steganography, steganography in streaming media, synchronization of video and audio, password protection, intellectual property protection, medical applications, military communication, fingerprinting, digital imaging, law enforcement, smart identity cards, media database systems, research, etc.[22]

## RESULTS AND DISCUSSIONS

Steganography for images can be enhanced and used more widely. Steganography can be used as the framework of an application to transmit messages secretly. Also, it can be used as a tool in different messaging apps, an icon for the steganographic job. Upon clicking that icon, a user interface opens that allows you to embed steganographic text into an image and transmit it to the recipient. The recipient can then view the information via a user interface that requires a password.

## CONCLUSION

Image steganography is the practice of encrypting, such as text, graphics, or recordings, inside a cover image.

Traditional methods such as least significant bit substitution, A combination of discrete wavelet transformation (DWT) and discrete cosine transformation (DCT) and Pixel Value Differencing (PVD) technique are used. CNN models, which emerged from the encoder-decoder design, have a significant impact on image steganography. The encoder requires both the cover picture and the hidden image as input to create the stego image. A subgroup of general adversarial networks are deep CNNs. A GAN makes use of game theory to train generative models for adversarial image generation issues. By loading various tools, we have used Python to build image steganography and a user-friendly GUI. The device performs both the encoding and decoding of picture data. 7-zip is used to implement image steganography in a simpler method. Businesses and groups across the globe struggle with the problem of data theft on a daily basis. As communication technology develops, data corruption becomes more probable. Steganography for pictures can be improved and applied more frequently. Steganography can be used as the foundation of a programme to send information covertly.

## REFERENCE

[1] Subramanian, Nandhini, et al. "Image steganography: A review of the recent advances." *IEEE access* 9 (2021): 23409-23423.

[2] Kazi, Jawwad A. R., et al. "A novel approach to Steganography using pixel-based algorithm in image hiding." *2020 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 2020.

[3] Ansari, Arshiya S., Mohammad S. Mohammadi, and Mohammad Tanvir Parvez. "A multiple-format steganography algorithm for color images." *IEEE Access* 8 (2020): 83926-83939.

[4] Saleh, Mohammed A. "Image steganography techniques-a review paper." *International Journal of Advanced Research in Computer and Communication Engineering, ISSN* (2018): 2278-1021.

[5] Online: https://www.geeksforgeeks.org/image-steganography-in-cryptography/

[6] Online: https://www.simplilearn.com/what-is-steganography-article

[7]: online: https://www.edureka.co/blog/steganography-tutorial

[8]: Chaudhary, Dev Kumar, Sandeep Srivastava, and Tanupriya Choudhury. "Steganography for Confidential Communication and Secret Data storage." *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)*. IEEE, 2018.

[9] Johnson, Neil F., and Sushil Jajodia. "Exploring steganography: Seeing the unseen." *Computer* 31.2 (1998): 26-34.

[10] Gupta, Shilpa, Geeta Gujral, and Neha Aggarwal. "Enhanced least significant bit algorithm for image steganography." *IJCEM International Journal of Computational Engineering & Management* 15.4 (2012): 40-42.

[11] Mstafa, Ramadhan J., Khaled M. Elleithy, and Eman Abdelfattah. "A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC." *IEEE access* 5 (2017): 5354-5365.

[12] Swain, Gandharba. "Very high capacity image steganography technique using quotient value differencing and LSB substitution." *Arabian Journal for Science and Engineering* 44.4 (2019): 2995-3004.

[13] Duan, Xintao, et al. "Reversible image steganography scheme based on a U-Net structure." *IEEE Access* 7 (2019): 9314-9323.

[14] Van, Toan Pham, Thoi Hoang Dinh, and Ta Minh Thanh. "Simultaneous convolutional neural network for highly efficient image steganography." *2019 19Th international symposium on communications and information technologies (ISCIT)*. IEEE, 2019.

[15] Yang, Kuan, et al. "Provably secure generative steganography based on autoregressive model." *Digital Forensics and Watermarking: 17th International Workshop, IWDW 2018, Jeju Island, Korea, October 22-24, 2018, Proceedings*. Cham: Springer International Publishing, 2019.

[16] Van, Toan Pham, Thoi Hoang Dinh, and Ta Minh Thanh. "Simultaneous convolutional neural network for highly efficient image steganography." *2019 19Th international symposium on communications and information technologies (ISCIT)*. IEEE, 2019.

[17] Wu, Pin, Yang Yang, and Xiaoqiang Li. "Image-into-image steganography using deep convolutional network." *Advances in Multimedia Information Processing–PCM 2018: 19th Pacific-Rim Conference on Multimedia, Hefei, China, September 21-22, 2018, Proceedings, Part II 19*. Springer International Publishing, 2018.

[18] Wu, Pin, Yang Yang, and Xiaoqiang Li. "Stegnet: Mega image steganography capacity with deep convolutional network." *Future Internet* 10.6 (2018): 54.

[19] Goodfellow, Ian, et al. "Generative adversarial networks." *Communications of the ACM* 63.11 (2020): 139-144.

[20] Herrera Montano, Isabel, et al. "Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat." *Cluster Computing* 25.6 (2022): 4289-4302.

[21]Online:https://searchinform.com/challenges/information-security/information-security-analytics/information-leaks/information-leakage-cases/consequences-of-information-leakage/

[22] Online: https://www.researchgate.net/figure/Applications-of-steganography_fig8_344949733