STEGANOGRAPHY

14th Sep 2022

OVERVIEW

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content. The content to be concealed through steganography -- called *hidden text* -- is often encrypted before being incorporated into the innocuous-seeming *cover text* file or data stream. If not encrypted, the hidden text is commonly processed in some way to increase the difficulty of detecting the secret content.

Different Types of Steganography

1. Text Steganography − There is steganography in text files, which entails secretly storing information. In this method, the hidden data is encoded into the letter of each word.

2. Image Steganography − The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

3. Audio Steganography − It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier"). Its typical uses involve media playback, primarily audio clips.

4. Video Steganography − Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

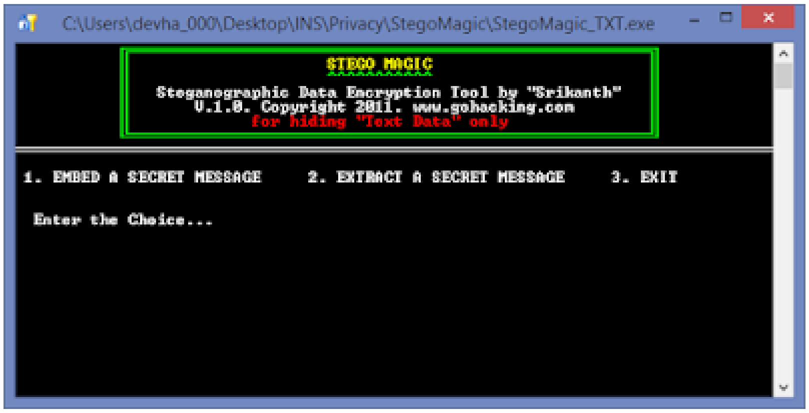
5. Network or Protocol Steganography − It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object. Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

Steganography using StegoMagic

It is a steganography tool that **implements intelligent algorithms to carefully embed the encrypted text messages or data inside other larger files such as an image, audio, video or an executable file**.

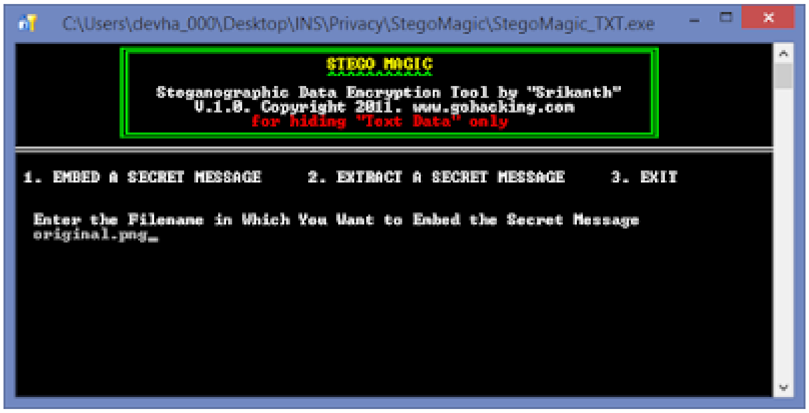
- All the files used in the process must be present in the local directory (folder) from which the StegoMagic tool is executed.
- You need to type the filenames along with the extension. Otherwise, you will receive an error message.
- For example,
- abc.jpg, nature.jpg, file.exe, cartoon.gif, video.avi etc.
- Use StegoMagic_TXT.exe to hide a text message inside any other file of your choice such as an image, video, sound or EXE file.
- Use StegoMagic_BIN.exe to hide one binary file in another.
- For example,
- You can hide a .jpg image in a .exe file or vice versa.
- You can use this tool (StegoMagic_BIN.exe) to hide any file of your choice in any other file. There are no limitations on what type of file can be hidden in one another. There are no limitations on the size of the file as well. So it is possible to hide a 1 GB video file in a 500 KB image file.
- Keep the "secret decryption key" safe which is required during the decryption process. The key will be displayed and a text file containing your secret decryption key will also be generated at the end of the encryption process.
- If you enter the wrong key during the decryption process, the output file generated will be of no use.
- NOTE: If you are using Windows 7 or 8 or 10, you need to run this tool as an administrator.

Step 1: Begin with encryption.


C:\Users\devha_000\Desktop\INS\Privacy\StegoMagic\StegoMagic_TXT.exe

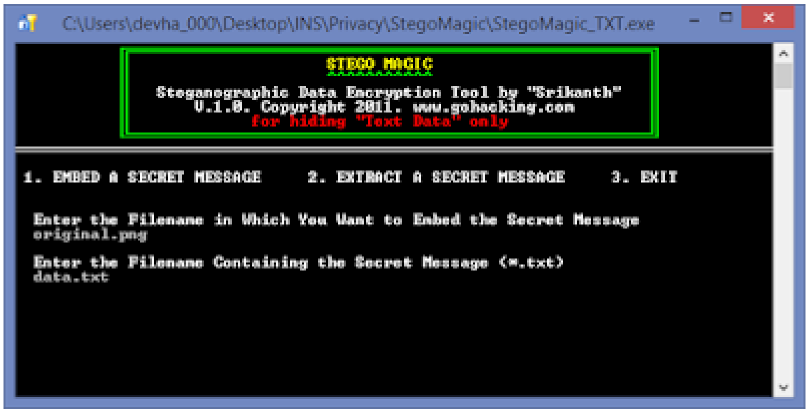
```
                         STEGO MAGIC
        Steganographic Data Encryption Tool by "Srikanth"
            V.1.0. Copyright 2011. www.gohacking.com
                  for hiding "Text Data" only

1. EMBED A SECRET MESSAGE      2. EXTRACT A SECRET MESSAGE      3. EXIT

 Enter the Choice...
```

Step 2: Select the image to process.


C:\Users\devha_000\Desktop\INS\Privacy\StegoMagic\StegoMagic_TXT.exe

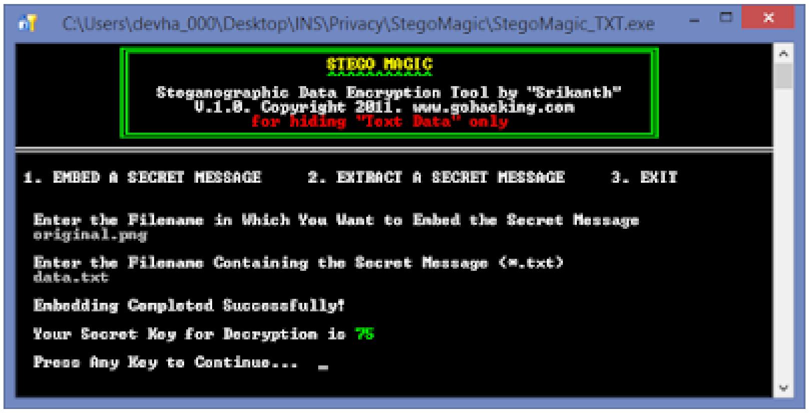
```
                         STEGO MAGIC
        Steganographic Data Encryption Tool by "Srikanth"
            V.1.0. Copyright 2011. www.gohacking.com
                  for hiding "Text Data" only

1. EMBED A SECRET MESSAGE      2. EXTRACT A SECRET MESSAGE      3. EXIT

 Enter the Filename in Which You Want to Embed the Secret Message
 original.png_
```

Step 3: Select data to hide.


C:\Users\devha_000\Desktop\INS\Privacy\StegoMagic\StegoMagic_TXT.exe

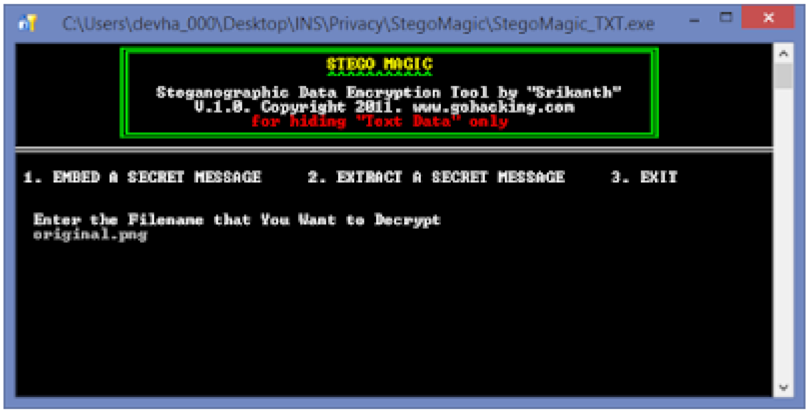
```
                         STEGO MAGIC
        Steganographic Data Encryption Tool by "Srikanth"
            V.1.0. Copyright 2011. www.gohacking.com
                  for hiding "Text Data" only

1. EMBED A SECRET MESSAGE      2. EXTRACT A SECRET MESSAGE      3. EXIT

 Enter the Filename in Which You Want to Embed the Secret Message
 original.png

 Enter the Filename Containing the Secret Message (*.txt)
 data.txt
```

Step 4: Data is hidden. Save the key.


C:\Users\devha_000\Desktop\INS\Privacy\StegoMagic\StegoMagic_TXT.exe

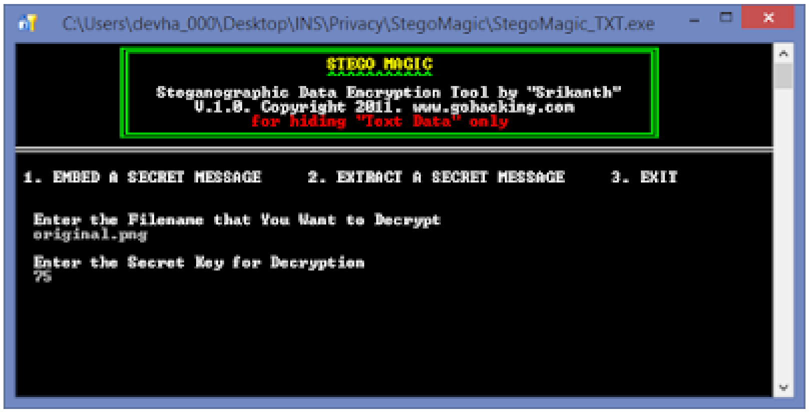
```
                    STEGO MAGIC
     Steganographic Data Encryption Tool by "Srikanth"
         V.1.0. Copyright 2011. www.gohacking.com
              for hiding "Text Data" only

1. EMBED A SECRET MESSAGE     2. EXTRACT A SECRET MESSAGE     3. EXIT

 Enter the Filename in Which You Want to Embed the Secret Message
 original.png

 Enter the Filename Containing the Secret Message (*.txt)
 data.txt

 Embedding Completed Successfully!

 Your Secret Key for Decryption is 75

 Press Any Key to Continue... _
```

Step 5: Start decoding and select the file to decode.


C:\Users\devha_000\Desktop\INS\Privacy\StegoMagic\StegoMagic_TXT.exe

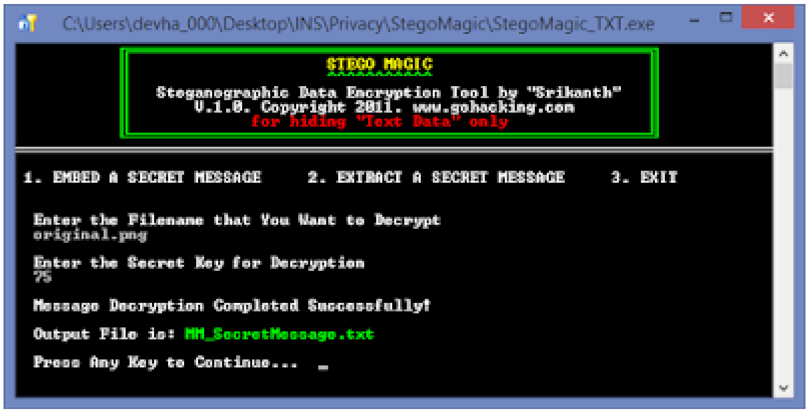
```
                    STEGO MAGIC
     Steganographic Data Encryption Tool by "Srikanth"
         V.1.0. Copyright 2011. www.gohacking.com
              for hiding "Text Data" only

1. EMBED A SECRET MESSAGE     2. EXTRACT A SECRET MESSAGE     3. EXIT

 Enter the Filename that You Want to Decrypt
 original.png
```

Step 6: Enter the password (decryption key).


C:\Users\devha_000\Desktop\INS\Privacy\StegoMagic\StegoMagic_TXT.exe

```
                    STEGO MAGIC
     Steganographic Data Encryption Tool by "Srikanth"
         V.1.0. Copyright 2011. www.gohacking.com
              for hiding "Text Data" only

1. EMBED A SECRET MESSAGE     2. EXTRACT A SECRET MESSAGE     3. EXIT

 Enter the Filename that You Want to Decrypt
 original.png

 Enter the Secret Key for Decryption
 75
```

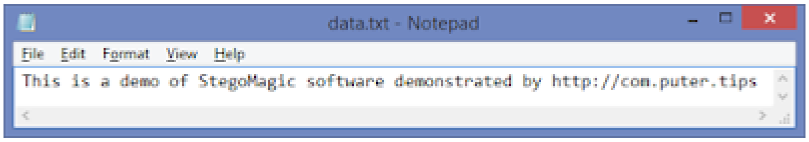
Step 7: Output is saved in the MM_SecretMessage.txt file.



C:\Users\devha_000\Desktop\INS\Privacy\StegoMagic\StegoMagic_TXT.exe

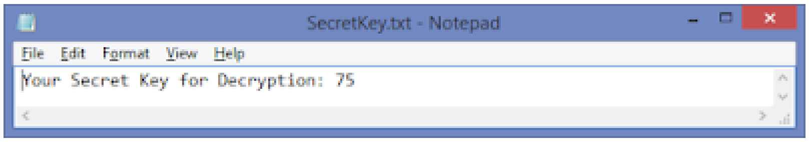
```
                          STEGO MAGIC
                          ~~~~~~~~~~~
        Steganographic Data Encryption Tool by "Srikanth"
              V.1.0. Copyright 2011. www.gohacking.com
                   for hiding "Text Data" only

1. EMBED A SECRET MESSAGE     2. EXTRACT A SECRET MESSAGE     3. EXIT

 Enter the Filename that You Want to Decrypt
 original.png

 Enter the Secret Key for Decryption
 75

 Message Decryption Completed Successfully!

 Output File is: MM_SecretMessage.txt

 Press Any Key to Continue...  _
```

A text file which was hidden:



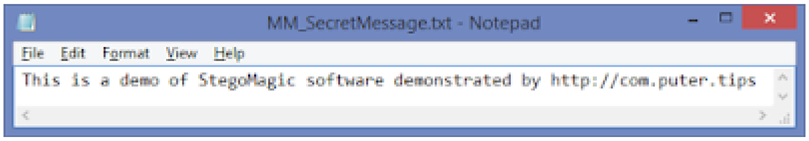
```
This is a demo of StegoMagic software demonstrated by http://com.puter.tips
```

Password (encryption/decryption key):



```
Your Secret Key for Decryption: 75
```

Information retrieved from the image:



```
This is a demo of StegoMagic software demonstrated by http://com.puter.tips
```