Kwantlen Polytechnic University

Foundation of Computer Security

Project

STEGANOGRAPHY

Instructor – Mandeep Pannu

Group Members

- Diksha Nagpal
- Jasmeen Kaur
- Kirandeep Sahota
- Anmolpreet Kaur
- Jaskaran Singh

Table of Contents

SR. NO.	TOPIC	PAGE NUMBER
1.	Subject Area	
2.	Abstract	
3.	Steganography types	
5.	Steganography tools	
6.	Steghide	
7.	SSuite Picsel	
8.	Open Puff	
9.		
10.	XIAO Steganography	
11.	Camouflage	
12.	Summary	
13.	Recommendations	
14.	References	

Subject Area

Confidential information has been exchanged among people since antiquity. Writing data on organisms' scalps and then shaving them again to extract the information was just one of the many methods that were employed. Methods of exchanging sensitive data must evolve considering changing technological conditions. Steganography is one of the best ways to do this after the massive success of cryptography. Forensic codebreaking is known as steganography. Hence, steganography is not only the art of concealing data, but it is also the art of concealing the fact that secret data is being transmitted.

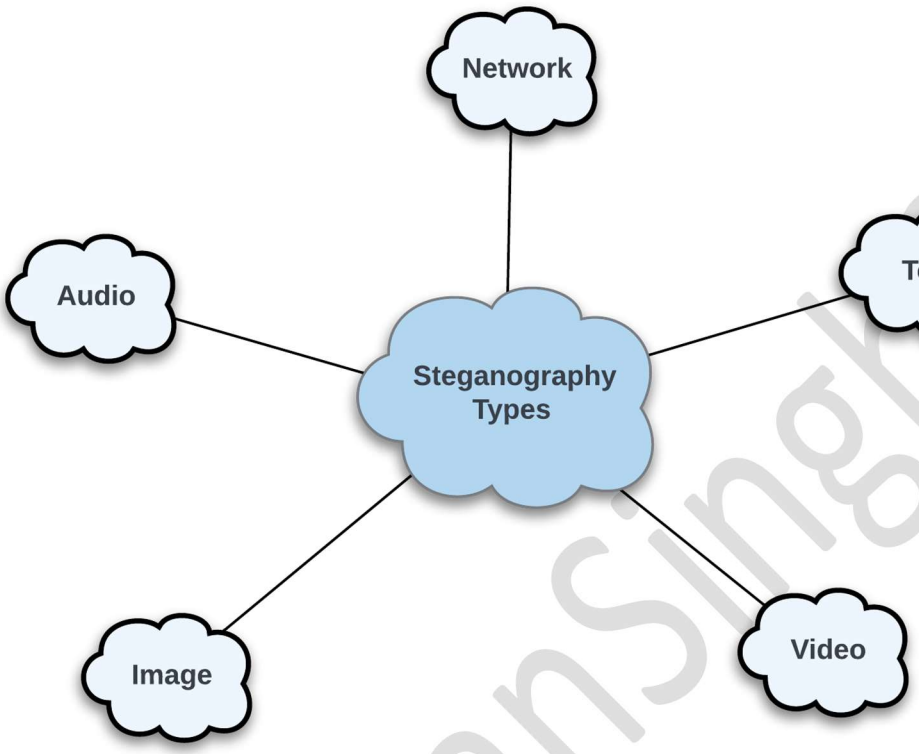
The secret file is hidden in another file using stenography, so only the person who gets it will know about it.

Abstract

“WAYS TO HIDING DATA WITH STEGANOGRAPHY”

Steganography is the study of encrypting and disguising data, such as images, audio, and video files, for transmission. Since it is presumed that the attack point is obvious if the feature is visible, hiding the embedded data is always a primary objective. There are numerous uses for steganography. However, it can be abused just like any other scientific method. As computing power has grown, so has awareness of the need of security among individuals, organisations, and governments, as well as via academic study and research. The primary differences between steganography and other related techniques, such as watermarking and cryptography, are its undetectability, robustness (resistance to various image processing methods and compression), and data capacity. This study presents a comprehensive review and analysis of the many steganographic techniques now in use, as well as some common guidelines for their implementation. Recommendations and citations are provided at the end of this publication.

Types of Steganography ways to hide the data:



➢ Text Steganography

Data may be hidden in text files using steganography. Text may be formatted in many ways, words within texts can be changed, words can be generated, and random letter sequences can be generated. It is possible to hide information in text in a variety of ways.

➢ Image Steganography

Data may be hidden in an image by using image steganography, which is a common method because of the considerable number of bits in digital representations of images as a result, images may be used to store or hide information.

Methods used to conceal data in images include the following.

1. Steganography with LSP.
2. Assembling a Masking and Filtering

➢ Audio Steganography

Coded messages are hidden inside audio signals that modify the binary sequence of associated files in this sort of steganography. Rather, it is a branch of study that deals with the art of encrypting a host communication with hidden text or audio.

➢ Video Steganography

With video steganography, any digital data may be concealed. This sort of steganography has the advantage of being able to hide a significant quantity of data.

Video steganography may be divided into two categories.

1. Embedding data in uncompressed raw video and then compressing it later.
2. Embedding data directly into a compressed data stream.

➢ Network Steganography

Network control protocols such as TCP, UDP, and ICMP can be used to hide information. As an example, the header TCP/IP packet might conceal information in fields that are either optional or of minor importance.

Steganography Tools:

1. Steghide
2. Openpuff
3. Stegosuite
4. SSuite Picsel
5. Camouflage

➢ Steghide

If you want to hide data in several types of image and audio files, you can use Steghide, which is a steganography programme. The frequency of each colour or sample is not changed, which makes the embedding resistant to first-order statistical tests, as shown in the figure.

- BMP, GIF and JPG supported
- Decryption via password
- Encryption of embedded data
- Uses various algorithms for encryption
- Compression of embedded data

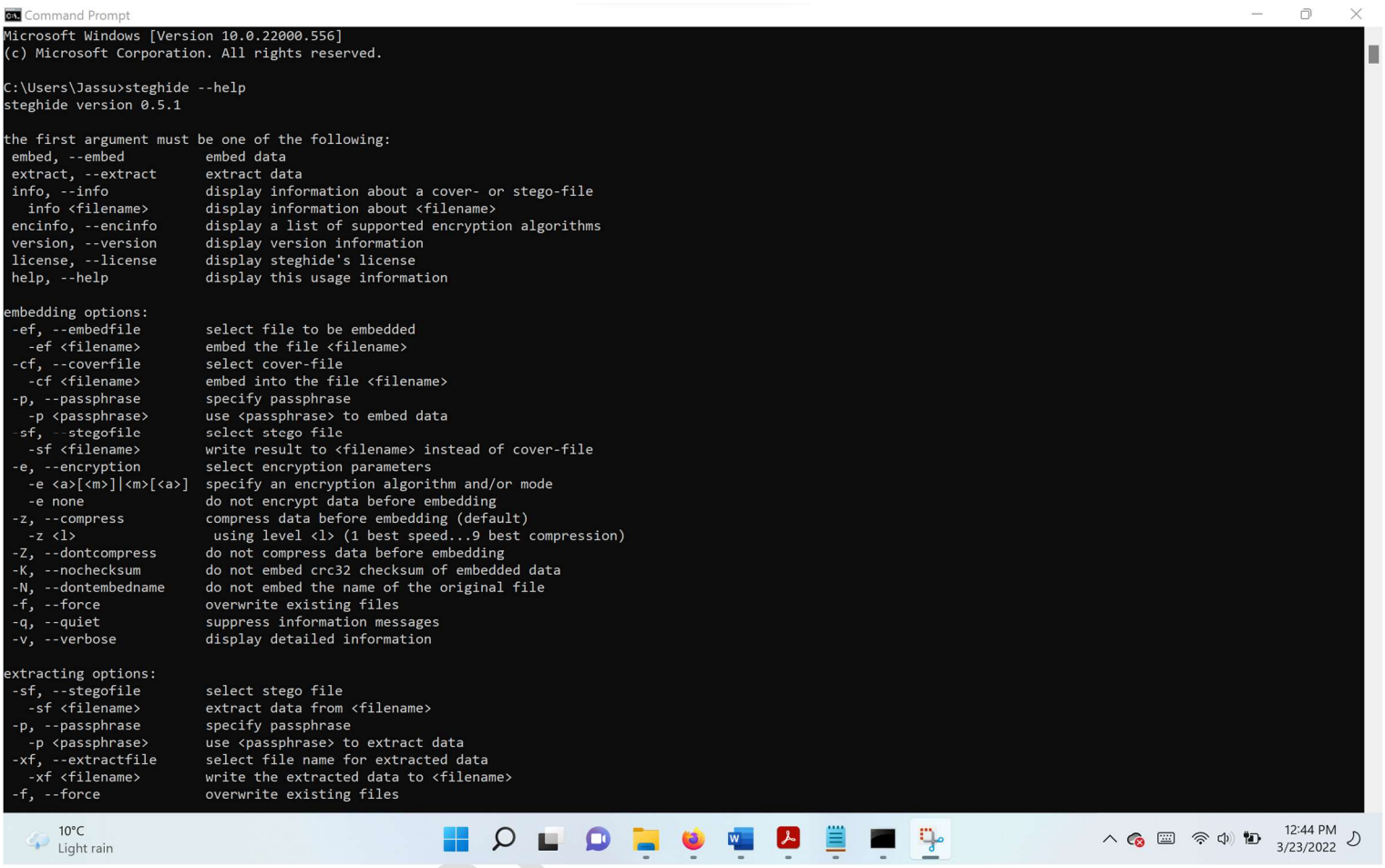
How to install stegohide:

Starting with the installation of Steghide, let us go ahead and do that. If we want to download stegohide in Windows, we can go to https://sourceforge.net/projects/steghide/ . Downloading and unzipping the files is all we need to do. We can then use the command prompt to get the files. Moreover, we must carefully copy the path of stegohide folder in environment variables to get their library files.

Commands:

The first basic command for getting the information about Stegohide is:

Steghide --help



- **How to embed the data in the Image:**

Steghide embed -ef <filename> -cf <filename>

Were,

ef is embed the file.

cf is cover the file.

```
C:\Users\Jassu>steghide embed -ef "C:\Users\Jassu\Desktop\FIles\New Text Document.txt" -cf C:\Users\Jassu\Desktop\FIles\jack.jpg
Enter passphrase:
Re-Enter passphrase:
embedding "C:\Users\Jassu\Desktop\FIles\New Text Document.txt" in "C:\Users\Jassu\Desktop\FIles\jack.jpg"... done
```

Passphrase is password, which we can later to retrieve the information back from it.

- **Command for retrieve the data back**

Steghide extract -sf <filename>

```
C:\Users\Jassu>steghide extract -sf C:\Users\Jassu\Desktop\FIles\jack.jpg
Enter passphrase:
wrote extracted data to "New Text Document.txt".
```

We can also use password protected commands for embed the file:

Steghide embed -ef <filename> -cf <filename> -p <password>

```
C:\Users\Jassu>steghide embed -ef "C:\Users\Jassu\Desktop\FIles\New Text Document.txt" -cf C:\Users\Jassu\Desktop\FIles\jack.jpg -p 971
embedding "C:\Users\Jassu\Desktop\FIles\New Text Document.txt" in "C:\Users\Jassu\Desktop\FIles\jack.jpg"... done
```

- **Retrieve back data from password protected file:**

  Steghide extract -sf <filename> -p 971

```
C:\Users\Jassu>steghide extract -sf C:\Users\Jassu\Desktop\FIles\jack.jpg -p 971
the file "New Text Document.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "New Text Document.txt".
```

- **We can also use Compression mode:**

  Steghide embed -ef <filename> -cf <filename> -z 2

The level of compressions is from 1 to 9, whereas first digits give competitive speed for the compression while last digits give best result for compress the file.

```
C:\Users\Jassu>steghide embed -ef C:\Users\Jassu\Desktop\FIles\Jassa.txt -cf C:\Users\Jassu\Desktop\FIles\jack.jpg -z 2
Enter passphrase:
Re-Enter passphrase:
embedding "C:\Users\Jassu\Desktop\FIles\Jassa.txt" in "C:\Users\Jassu\Desktop\FIles\jack.jpg"... done
```

- **Command to retrieve the information about the file**

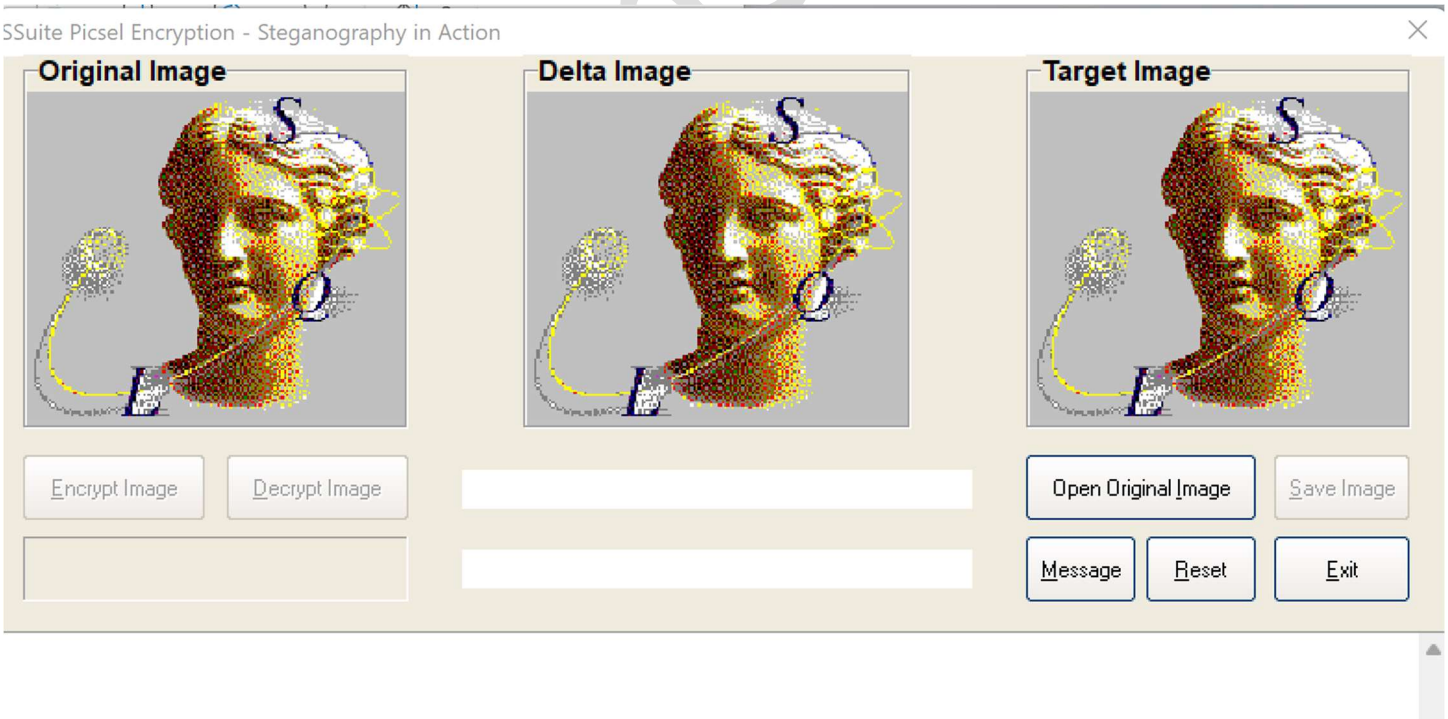
```
C:\Users\Jassu>steghide info C:\Users\Jassu\Desktop\FIles\jack.jpg
"jack.jpg":
  format: jpeg
  capacity: 36.5 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "New Text Document.txt":
    size: 13.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

SSuite Picsel

To conceal text files and handwritten text within images, SSuite Picsel was developed as a portable steganography tool. To protect your text data, it encrypts the image that you submit and allows you to decrypt it. A picture or message can be hidden within another image or message using this software's steganography technology. It is possible to insert a text file, a message, or a custom text into an image with this software. You must use the identical original image and encrypted image to recover the secret text. As a result, the original image serves as a password to unlock the hidden text.

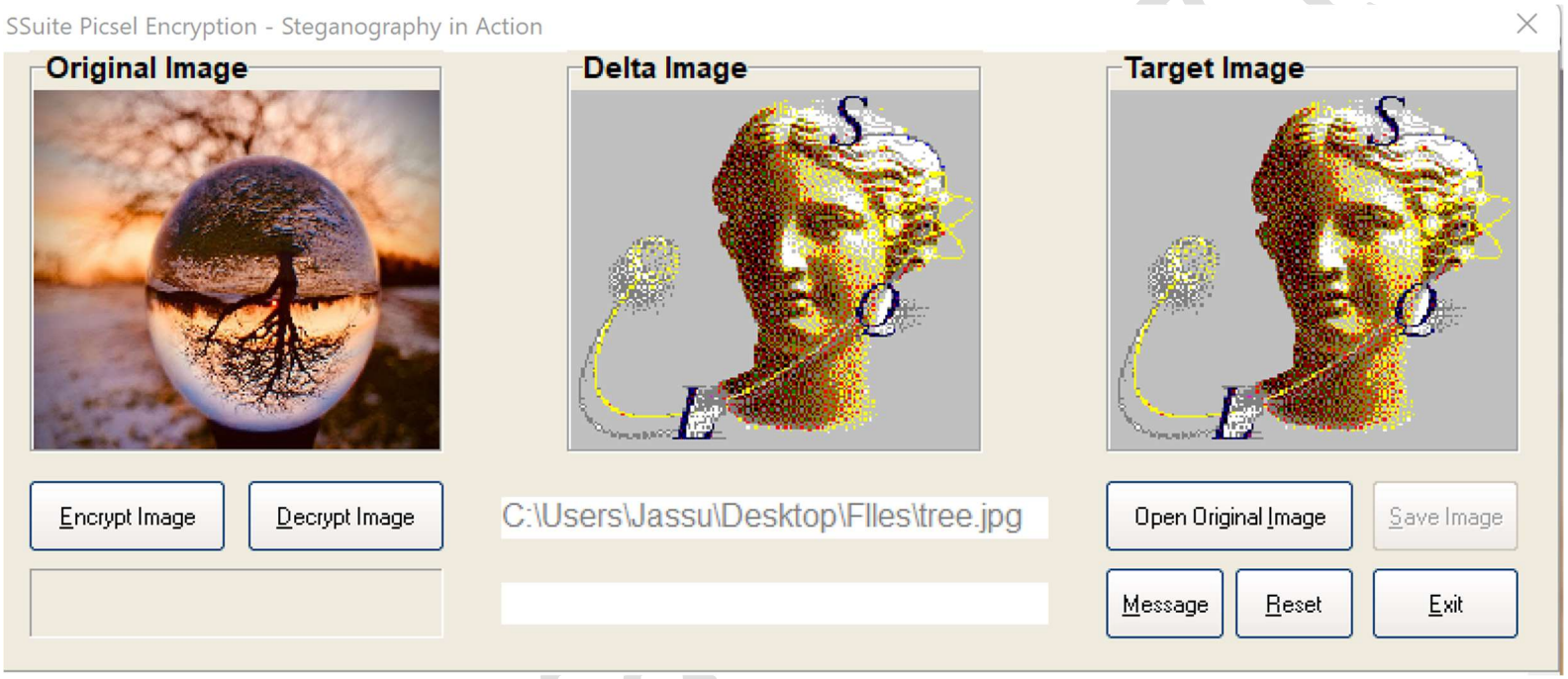
The encrypted image is identical to the original image. As a result, no one could argue that you stored any text data in that photograph. It can also come in handy when you need to send a secret message to a friend.

Interface Of SSuite Picsel



Steps to encrypt the file:

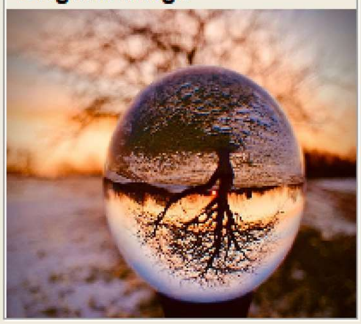
1. Primarily, we must select the image to whom we want to encrypt with the text file. Therefore, we must click on the open original Image where we can select the image. Now as we can see that Image as we can seen it in Original Image box.



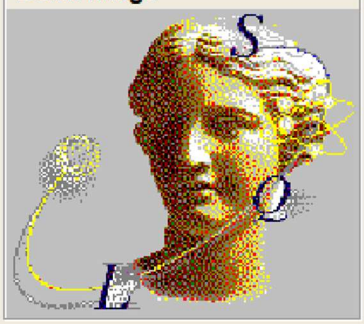
2. Next step is to select the word file to whom we want to hide behind the image. Therefore, we choose by clicking on Message button at the right behind.

SSuite Picsel Encryption - Steganography in Action

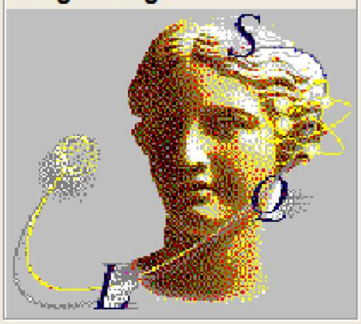
Original Image



Delta Image



Target Image



Encrypt Image | Decrypt Image

C:\Users\Jassu\Desktop\FIles\tree.jpg

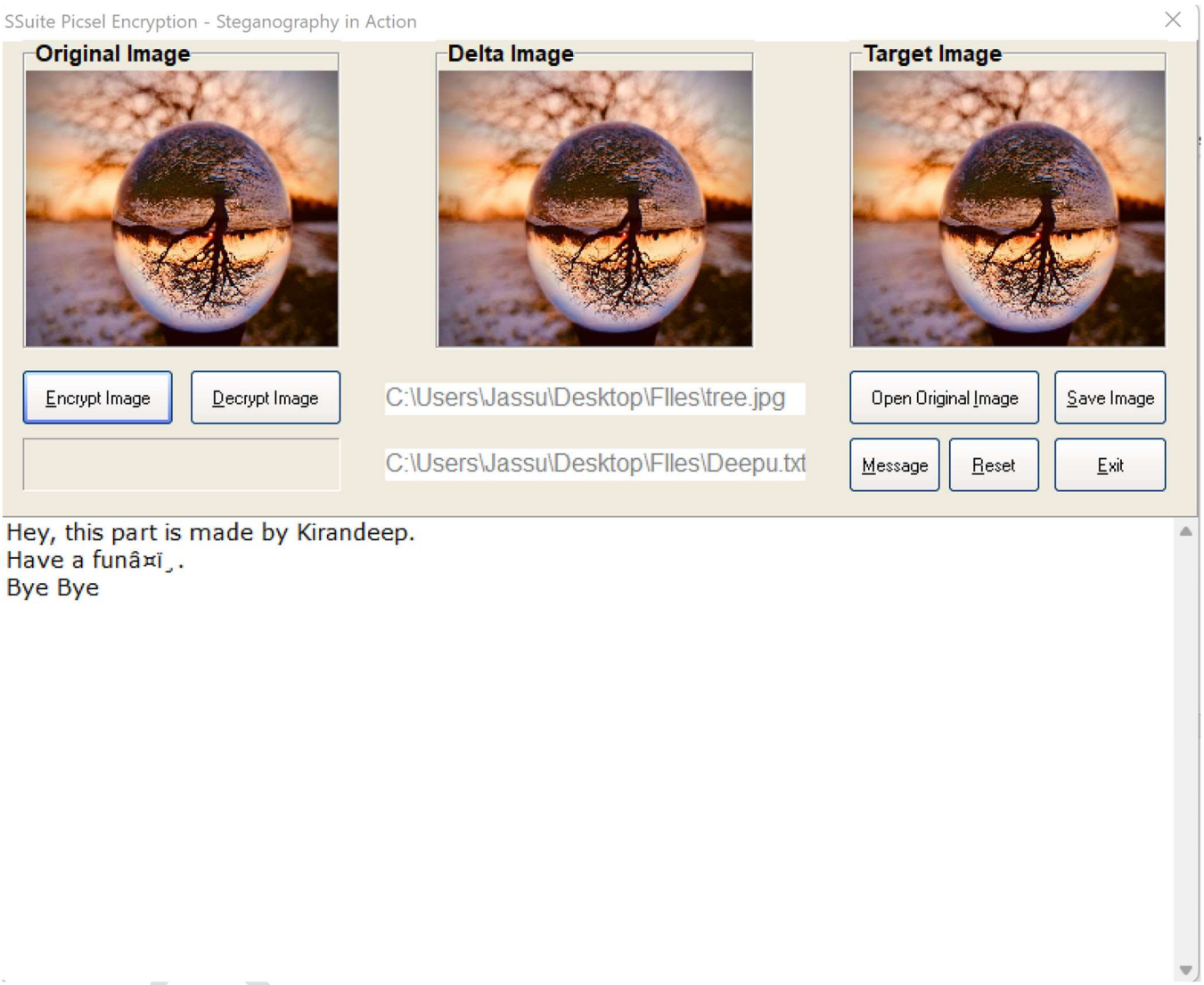
C:\Users\Jassu\Desktop\FIles\Deepu.txt

Open Original Image | Save Image

Message | Reset | Exit

Hey, this part is made by Kirandeep.
Have a funâ¤ï¸.
Bye Bye

3. Now, we must click on the encrypt the file, afterward it starts process the file and then encrypt the whole image with text.



4. At last, click on the save image and select the path where we want to save the file and enter the name of the file. So, file is encrypted.

SSuite Picsel is an intriguing and handy piece of software for hiding crucial text within an image. Even if someone discovers that you have saved the text, he or she will not be able to access the hidden text until the original image is returned to you. It is a clever way to conceal the text. I wish it could also support rtf, doc, and pdf files. However, it can only hide plain text files and custom messages.

How to decrypt the file:

In order to decrypt the file, we have to choose the encrypted file for the decrypt. Therefore, we choose the previous file that we made.

1. Click on the decrypted file then we have selected the path of encrypted file and choose the file.
2. Its starts decrypting then we get the words which were decrypted. Select the words then save it in the file.

3. Open Puff:

Open Puff is a professional steganography application with unique features that can be used to covertly transmit overly sensitive data.
Data is distributed among numerous carriers via Open Puff. Unhiding is only possible with the correct carrier sequence. Furthermore, if you have extra carriers, you can hide up to 256Mb. The final carrier will be loaded with random bits to blend in with the others.

Highlights and features:

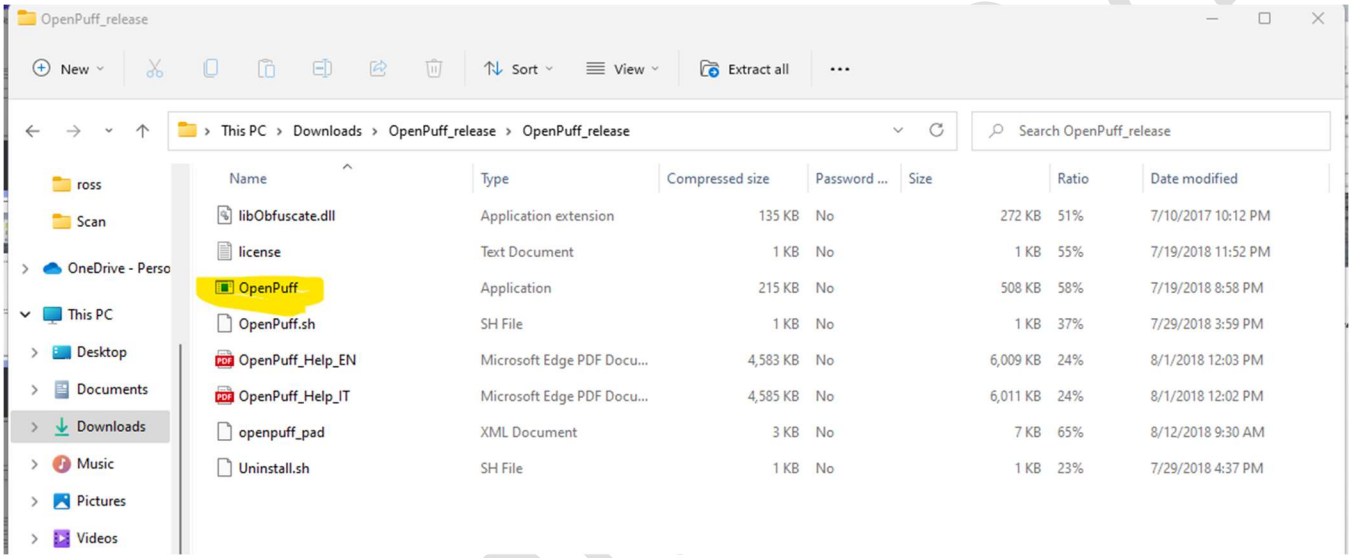
- Random number generator using HW seed (CSPRNG)
- Steganography that is undetectable
- Lines of communication (up to 256Mb of hidden data)
- Choosing the carrier bits
- Multi-cryptography is a technique used in modern times (16 algorithms)
- Data obfuscation in several layers (3 passwords)
- Resistance to x-squared steganalysis

Installation of Open Puff:

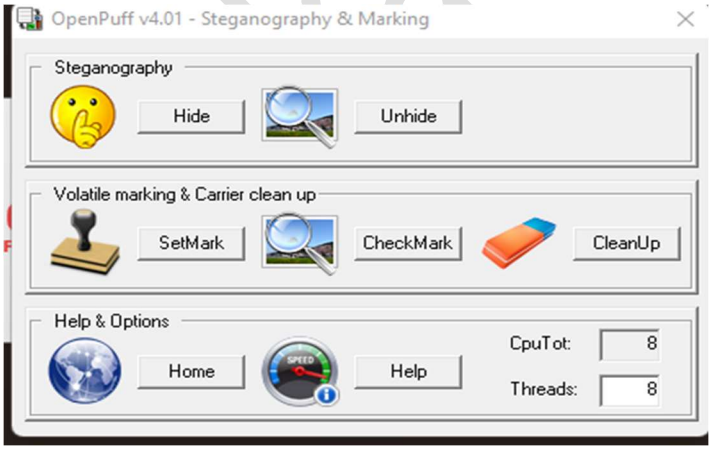
Because it is an open-source programme, you can get it from Google by clicking the link below.

https://embeddedsw.net/OpenPuff_download.html

It will be downloaded as a Zip folder. Open that folder and double-click openPuff.exe to bring up the window shown below.

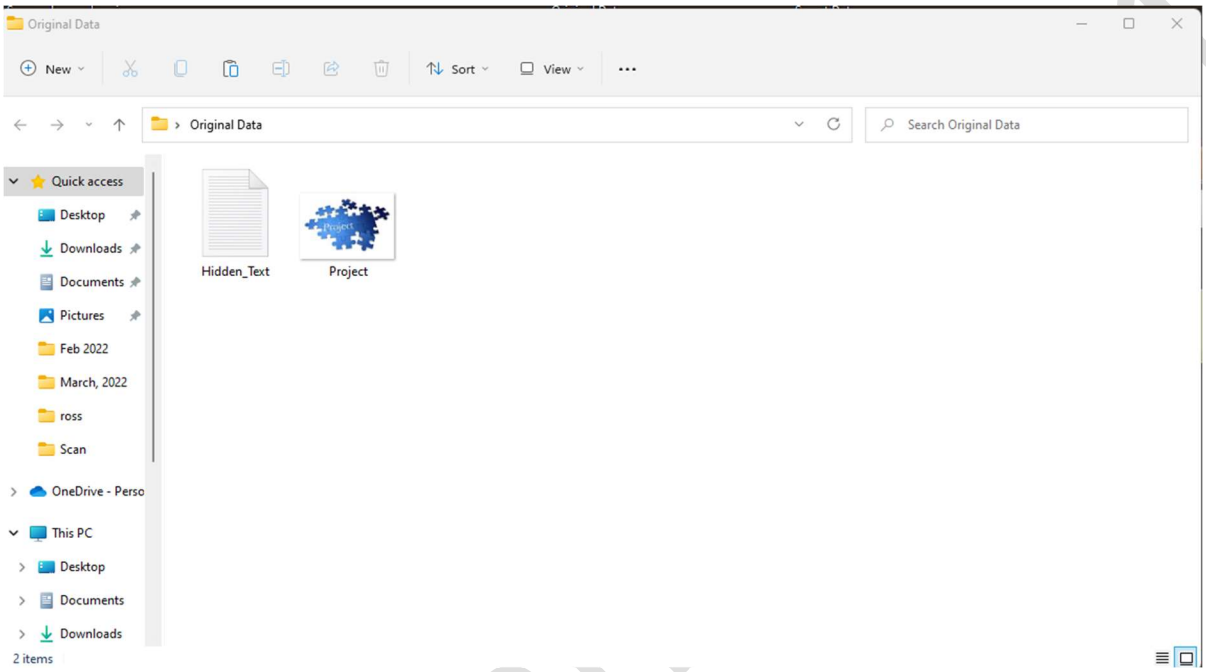


When you open the open.exe file you will see the interface of Open Puff.

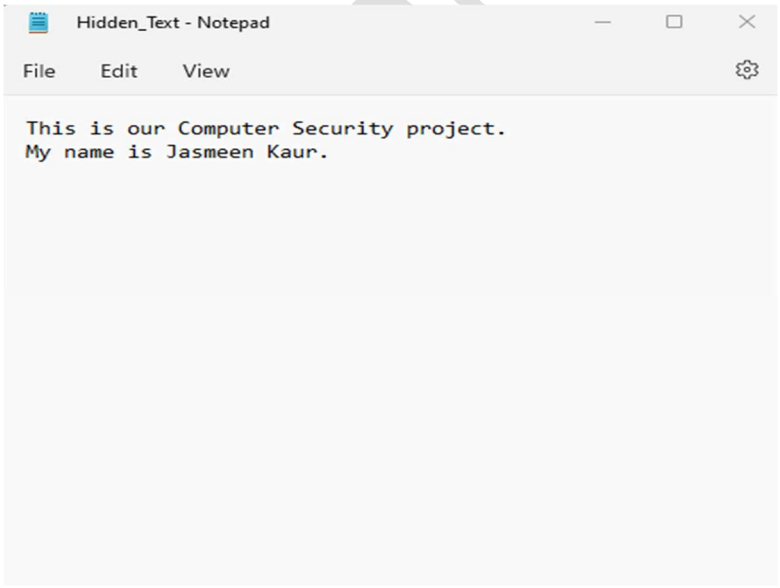


Begin the process by creating two folders on your desktop, one for "Original" and the other for "Secret."

You will find an image as well as your secret message or text file (project.jpg & Hidden_Text.txt) in the original folder. Using open Puff, you will hide a secret message in an image. As indicated in the screenshot below.



In the Hidden_Text.txt file, the secret text is “This is our Computer Security Project. My name is Jasmeen Kaur.”

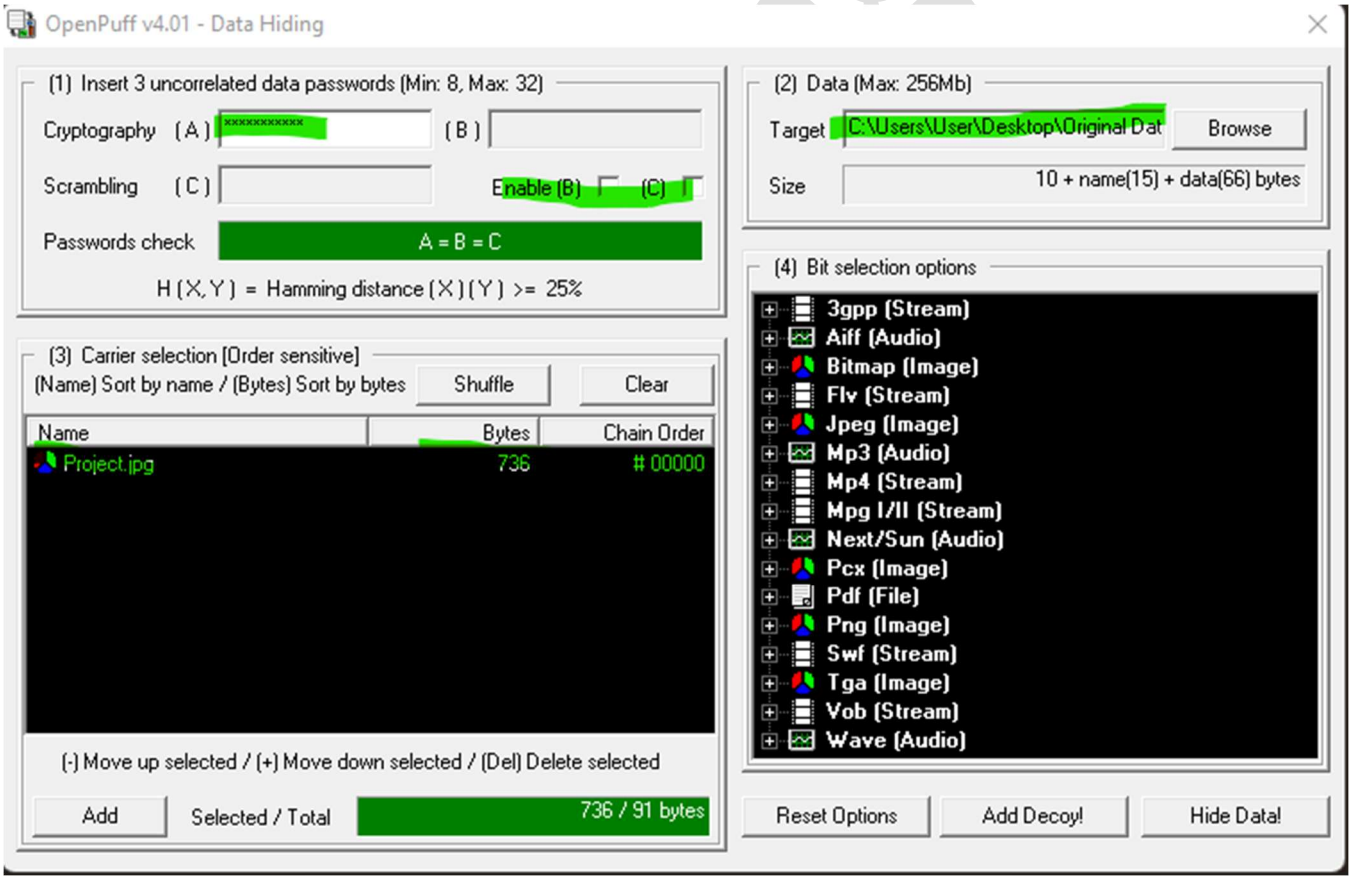


Encryption:

Return to the Open Puff now. Open this tool, select hide, and enter the secret message password. You must enter a password in the Cryptography (A) dialogue box, as seen below screenshot. Remember to uncheck the B and C boxes so you only must remember one password instead of three.

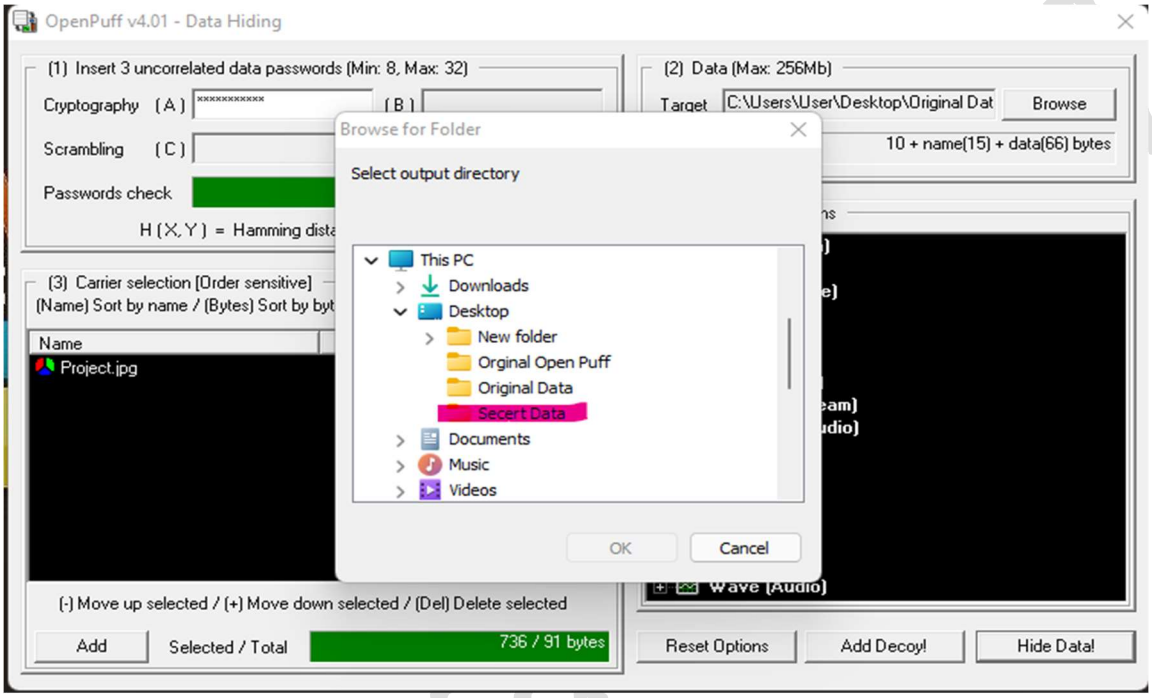
Then there will be a target option on the right-hand side, which will be the secret message file. Select the Hidden_Text.txt file by clicking on browse and going to the original folder.

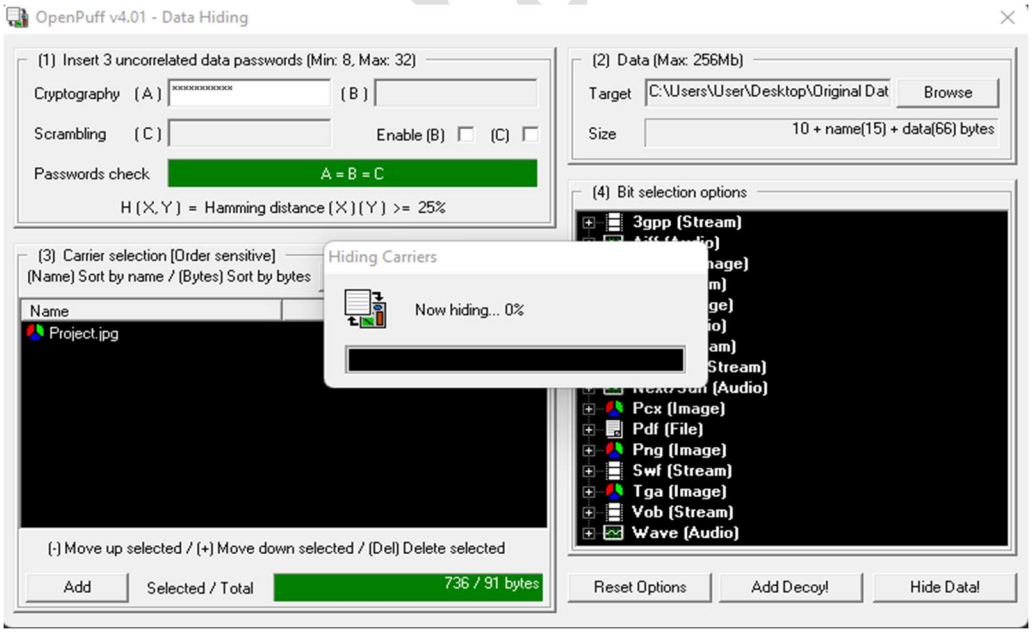
Then it is time to choose the carrier file which will carry the hidden information. That will be project.jpg image in our original folder. In open Puff tool on the below of the left side there will be Add button click on that, browse to the original folder, and choose the project.jpg as a carrier file.



After that, on the tool's right side, click Hide Data. A little window will appear on the screen as soon as you click the hide data button. Now, because our second folder's name is Secret, you must select the Secret option. Then, click Ok, and the Secret folder will appear.

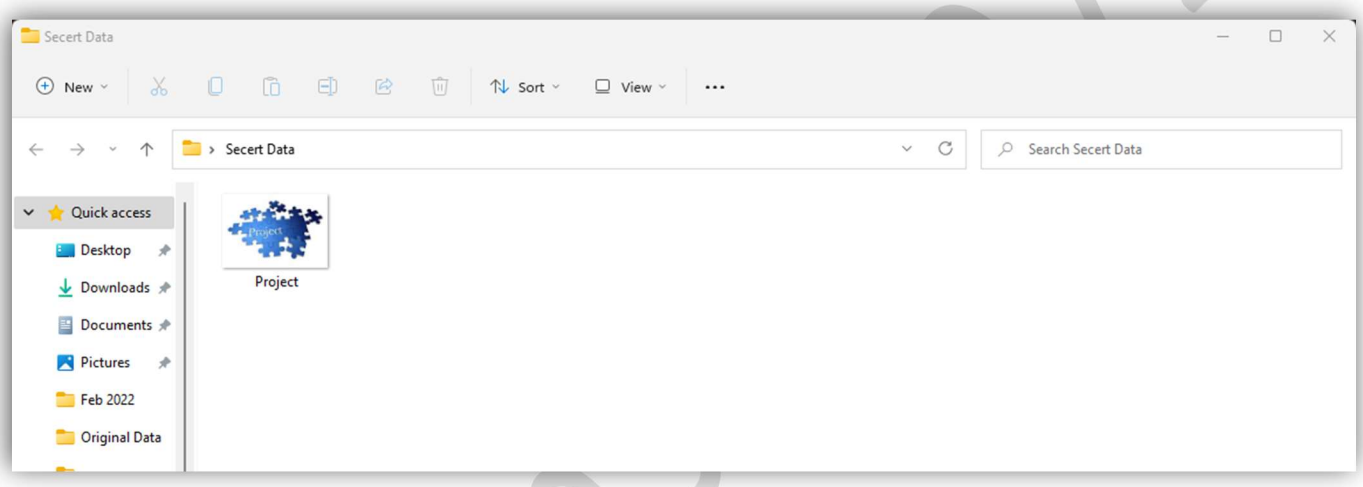
In your Secret labelled folder, there is a flower.jpg image with concealed secret information.





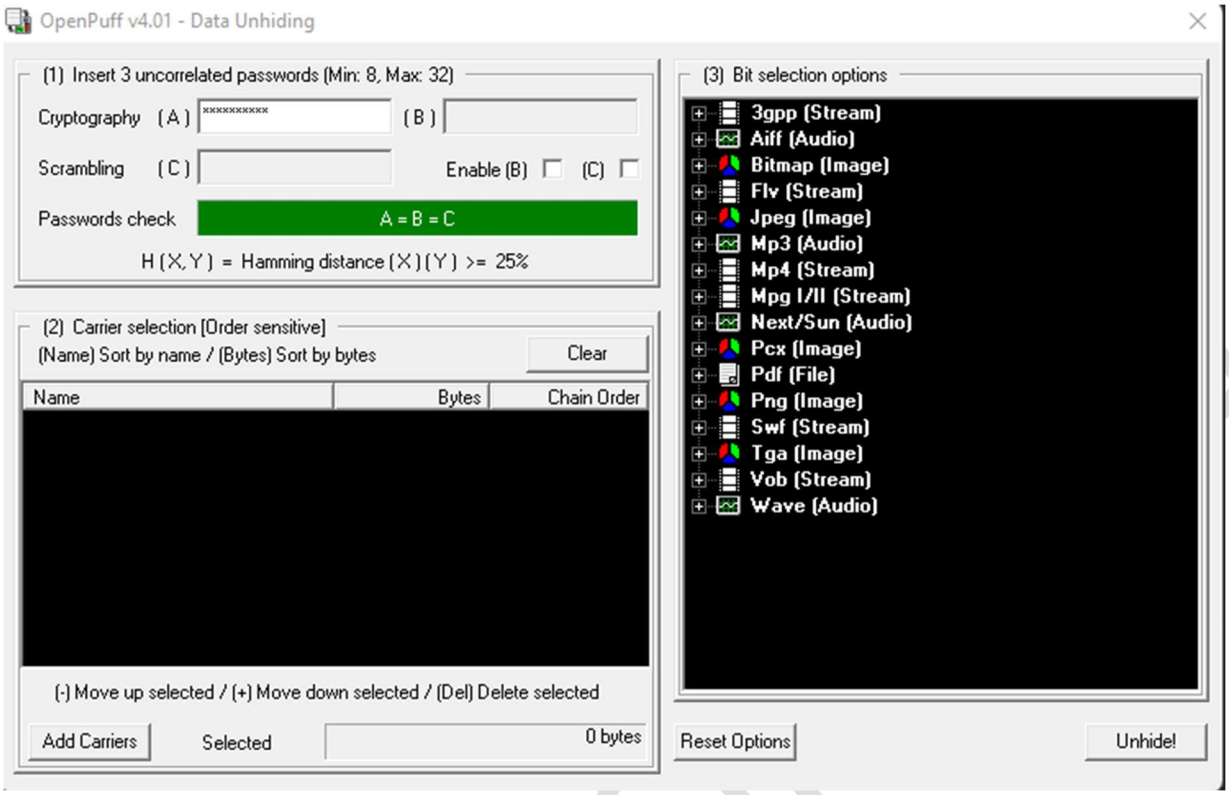
This is the end of hiding process.

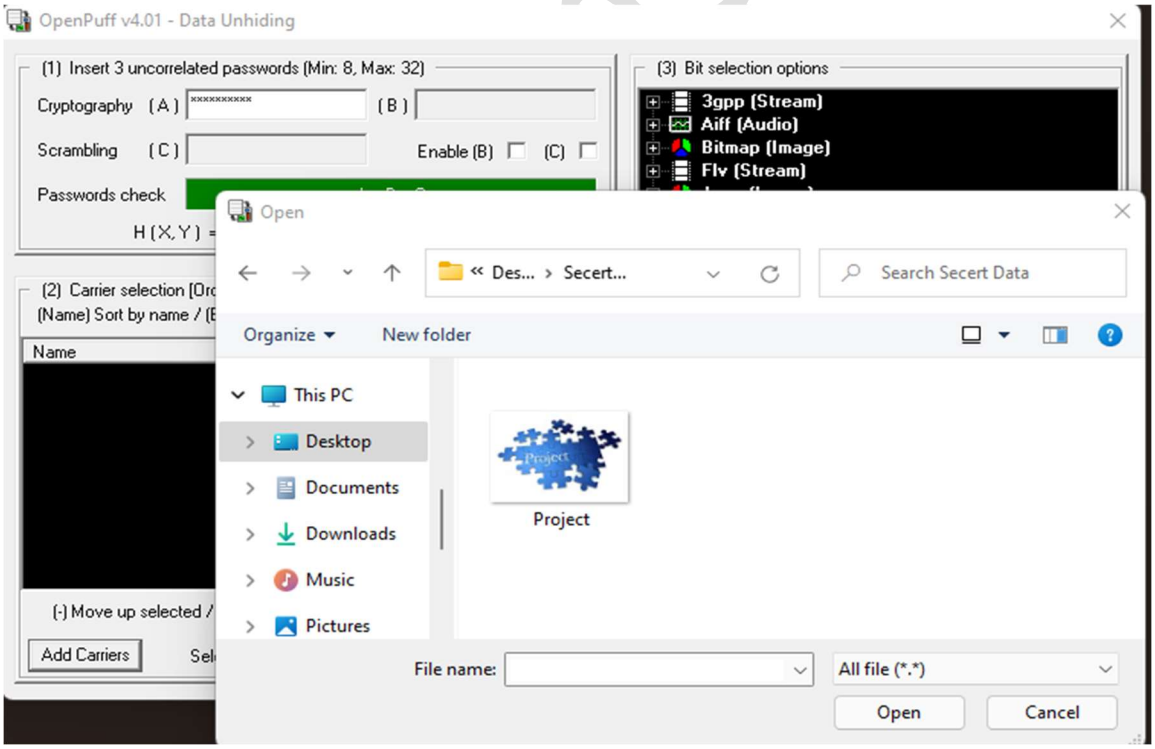
After Encryption Data:

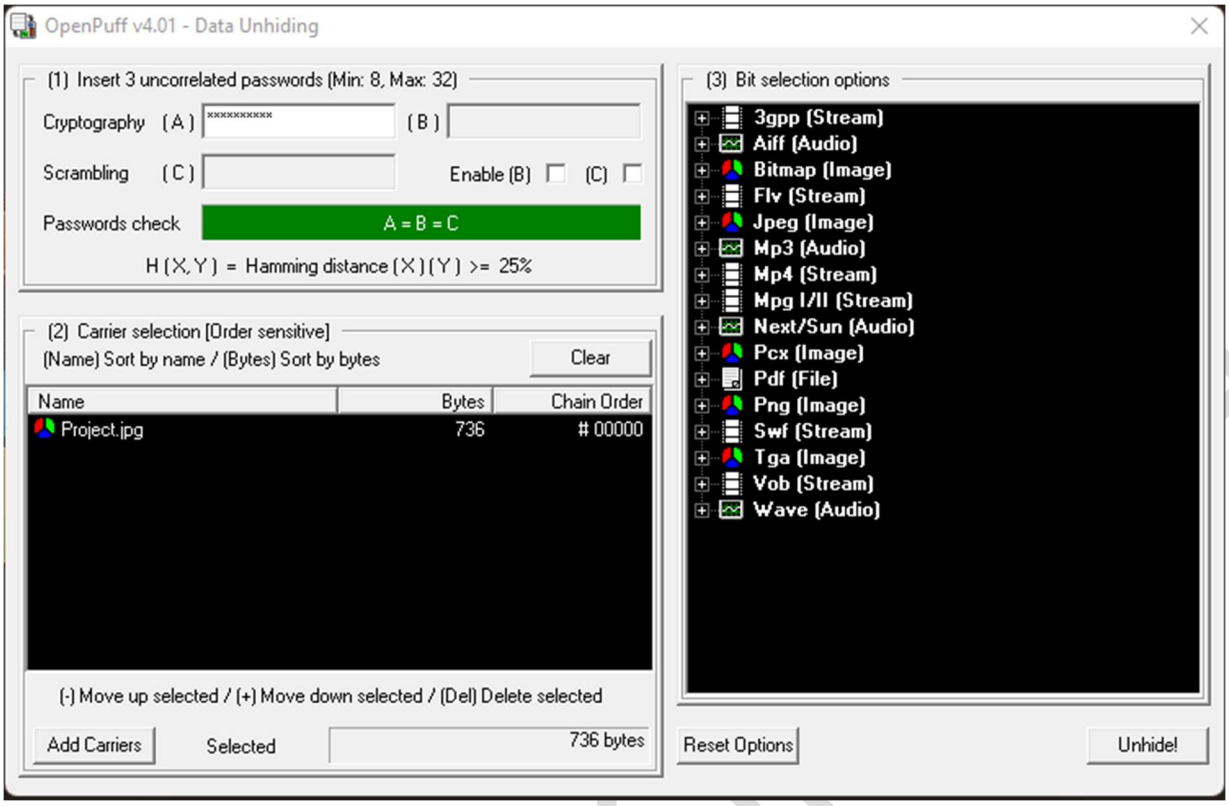


Decryption: In the process of decryption, you must unhide the secret message. In the same Open Puff window click on Unhide button. To complete the decryption process, you must write the same password that you entered encrypting. I entered "ComputerSecurity" password. So, I will use the same password. Uncheck the options B and C that we checked when masking data in the same way.

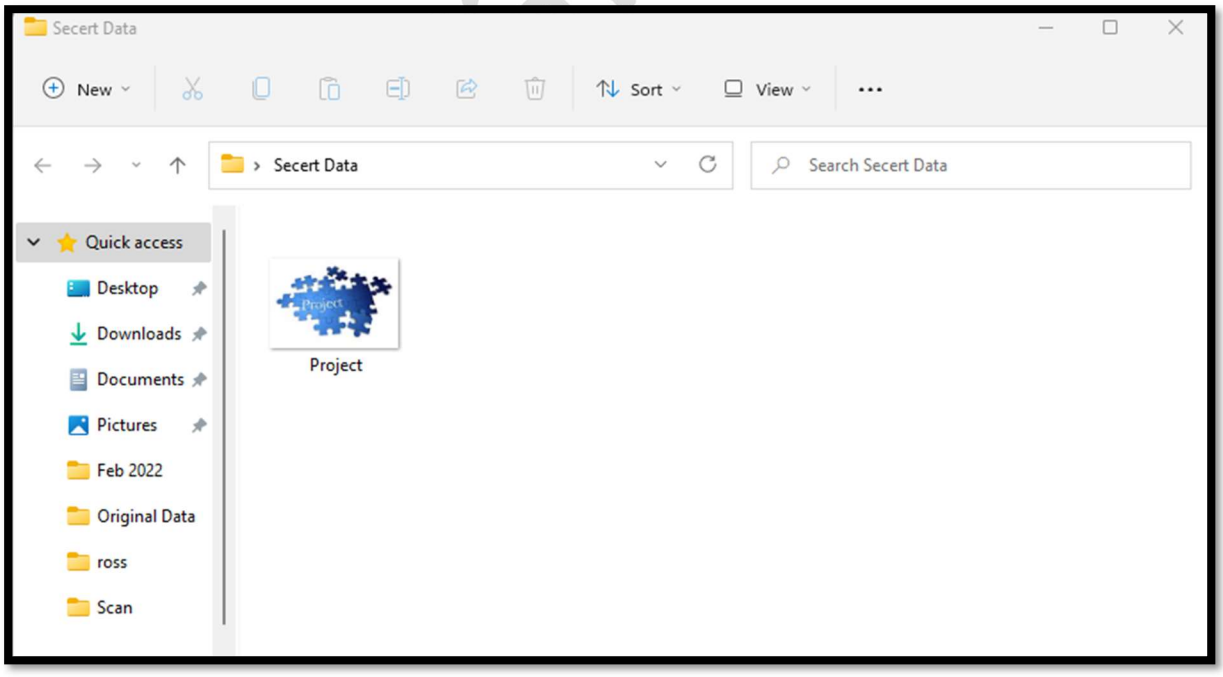
The carrier file will be flower.jpg from the secret folder, not from the original folder, this time. So, navigate to the secret folder on your desktop and select the project.jpg image file by clicking the Add button. After clicking on unhide, a little window will appear, prompting us to select the secret named folder and then click OK. After that, we are done with the decryption because the hidden.txt file will appear in your secret folder, indicating that we can now read the secret information.


OpenPuff v4.01 - Data Unhiding
(1) Insert 3 uncorrelated passwords (Min: 8, Max: 32)
Cryptography (A)
****
(B)
Scrambling (C)
Enable (B) (C)
Passwords check
A = B = C
H(X,Y) = Hamming distance(X)(Y) >= 25%
(2) Carrier selection [Order sensitive]
(Name) Sort by name / (Bytes) Sort by bytes
Clear
Name
Bytes
Chain Order
(-) Move up selected / (+) Move down selected / (Del) Delete selected
Add Carriers
Selected
0 bytes
(3) Bit selection options
3gpp (Stream)
Aiff (Audio)
Bitmap (Image)
Flv (Stream)
Jpeg (Image)
Mp3 (Audio)
Mp4 (Stream)
Mpg I/II (Stream)
Next/Sun (Audio)
Pcx (Image)
Pdf (File)
Png (Image)
Swf (Stream)
Tga (Image)
Vob (Stream)
Wave (Audio)
Reset Options
Unhide!


OpenPuff v4.01 - Data Unhiding
(1) Insert 3 uncorrelated passwords (Min: 8, Max: 32)
Cryptography (A)
****
(B)
Scrambling (C)
Enable (B) (C)
Passwords check
(3) Bit selection options
3gpp (Stream)
Aiff (Audio)
Bitmap (Image)
Flv (Stream)
Open
« Des... › Secert...
Search Secert Data
Organize
New folder
This PC
Desktop
Documents
Downloads
Music
Pictures
Project
File name:
All file (*.*)
Open
Cancel

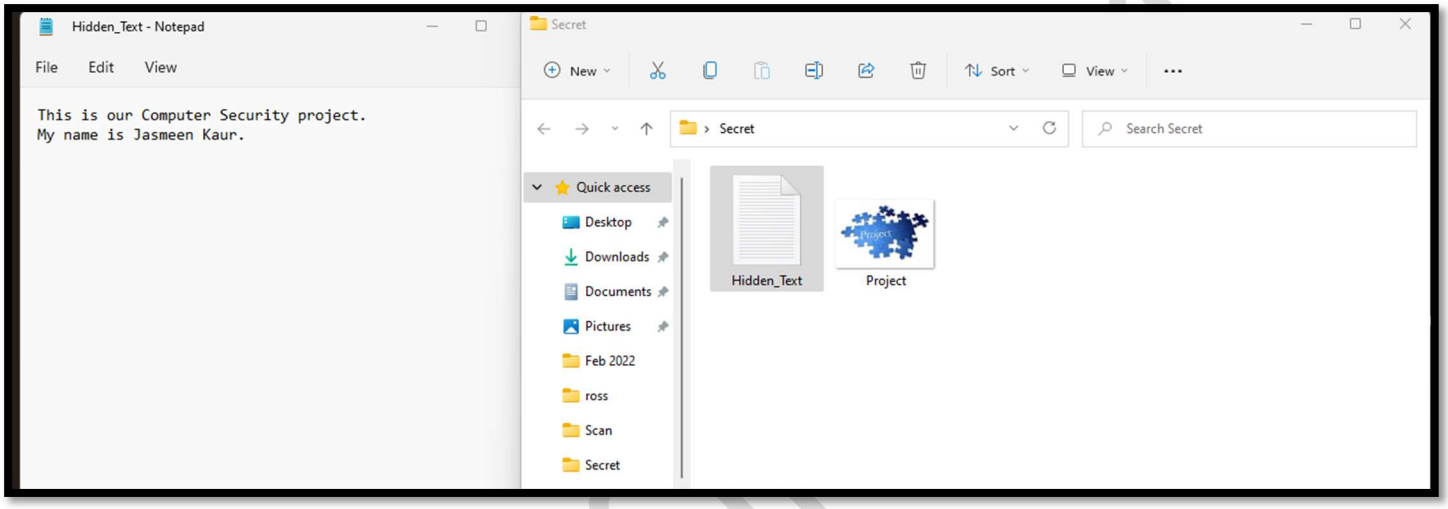


Before encryption:



We may now access the hidden information by opening the Hidden_Text.txt file after we've completed the decryption process.

After Encryption:



Camouflage

The steganography techniques before needed extensive planning and cooperation to gain success .But now a days it is easier than before we do not need to do that much as much, we use to The simple forms of steganography also limited the usefulness to the media in which they were implemented. With the rise in technology the ease of use in steganography has also increased so that any person with a computer and internet can do steganography .Camouflage Software id easy to use ,install , and a very versatile steganography tool that is free of charge and available for download to any . Software programs can be found in great numbers on the internet propagating material. Software has also become easier to use and more functional as the technology have gained success in very field. Steganography is just starting to emerge with more powerful and full featured programs. Many of the steganography programs are very simple to use but have limited capability in the files used for steganography purposes. Camouflage software is a program that has eliminated the need for graphics text files or any other specific source . This program software used to hide the information can use many techniques including insertion, injection, and substitution. Camouflage will take virtually is a camouflaged file that seems as a file used for this process.

REQUIREMENTS

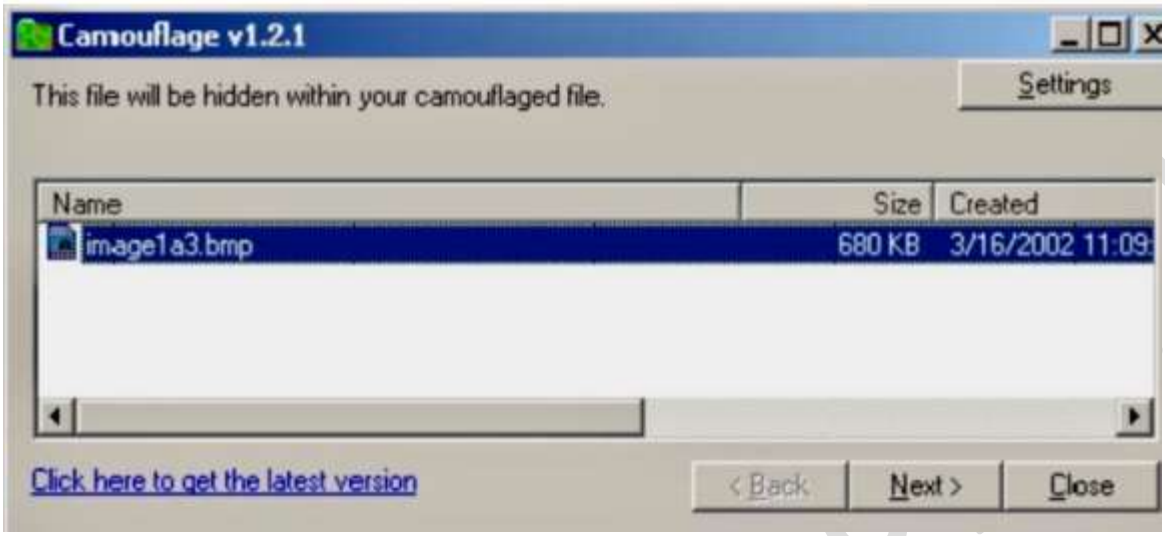
The ability to run a steganography program no longer requires special equipment ,extensive amounts of time or known shared keys . in the past ,all parties involved with a file that had hidden data had to be aware of the file and how it was hidden But today we do not need to do such acts .To download Camouflage you require Windows 95,Windows 98,Windows ME, Windows NT ,or Windows 200 minimum .Including these minimal requirements the hardware needed to use steganography is also abundantly available .The downloaded file comes as a Zipped folder that needs to be extracted by us .Camouflage is oriented to Windows operating system making the final requirements a simple browser program such as file manager or windows explorer.

INSTALLATION

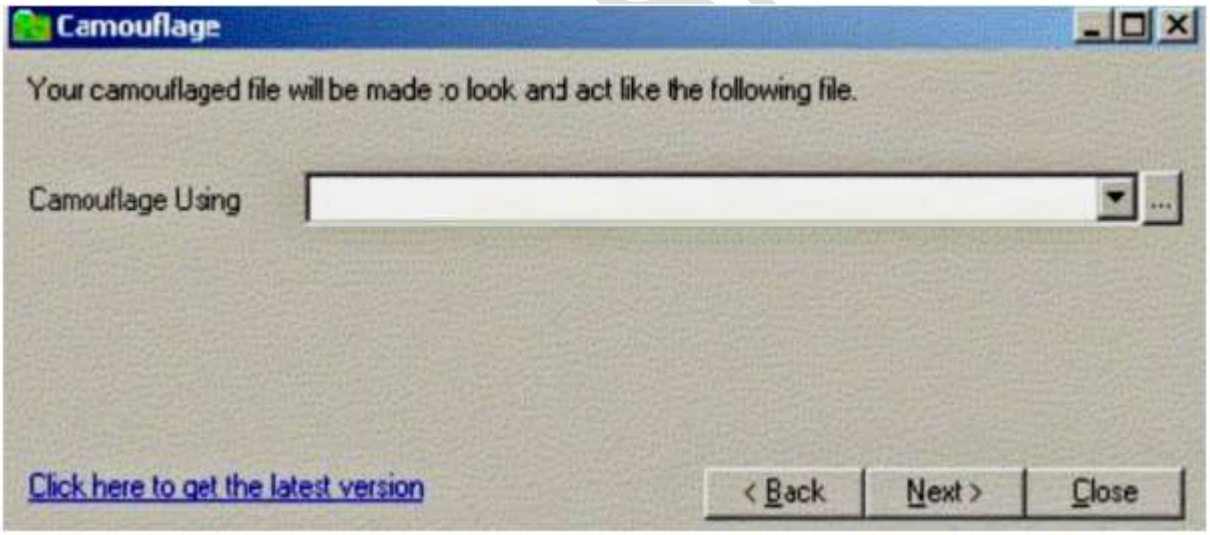
After downloading the file and extracting ,the Camouflage program is a self-executing file that will step through the installation process . the installation process will complete and will be operational with very little effort .Installation Takes no longer than 5 minutes and the capability to perform steganography have been added to the toolbox.

CAMOUFLAGING FILES

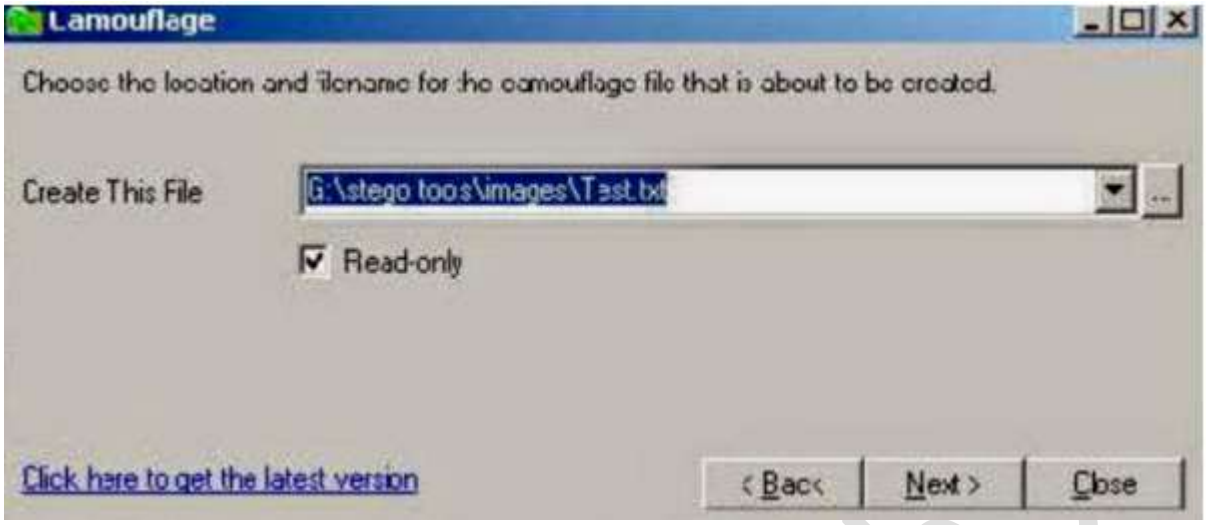
1) The Camouflage window as it appears after selecting a file to camouflage .



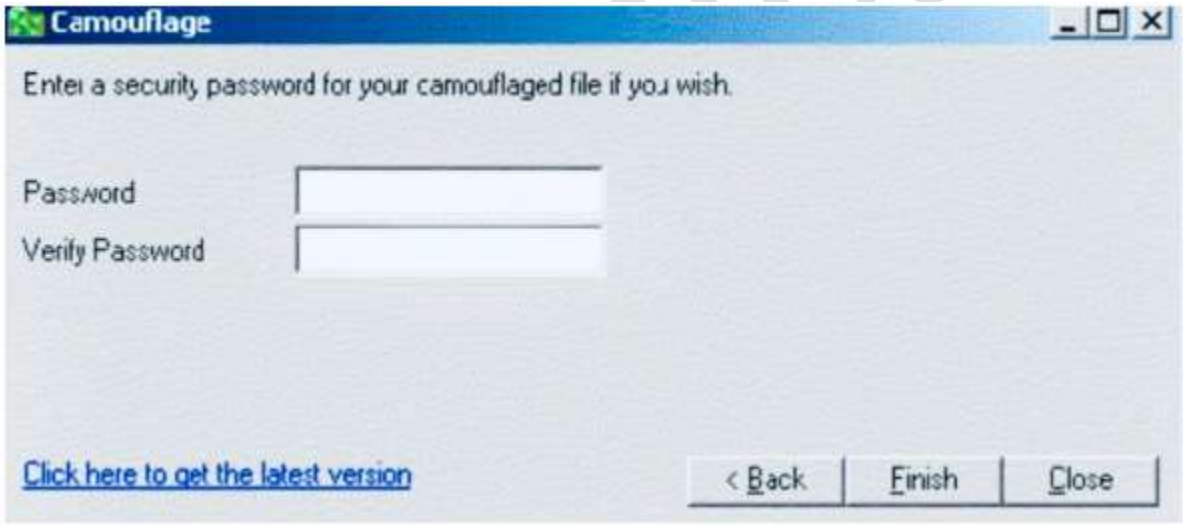
2) The image selected “image1a3.bmp” is the image that will be camouflaged in a file selected at a later step. The size of the image here is 680KB .Selecting next will bring up the file selection in which to embed the image.



3) Her the camouflage process using the next button to choose a file . The chosen file can be virtually of any type and does not require any consistency. After selecting a file , the option Rename the new camouflaged file will appear .Note in the figure there are two key items that are important . One the name of the new file is not to be associated with the original file .Two the ability to verify file is read only is once again presented to ensure corruption of the file will not occur .



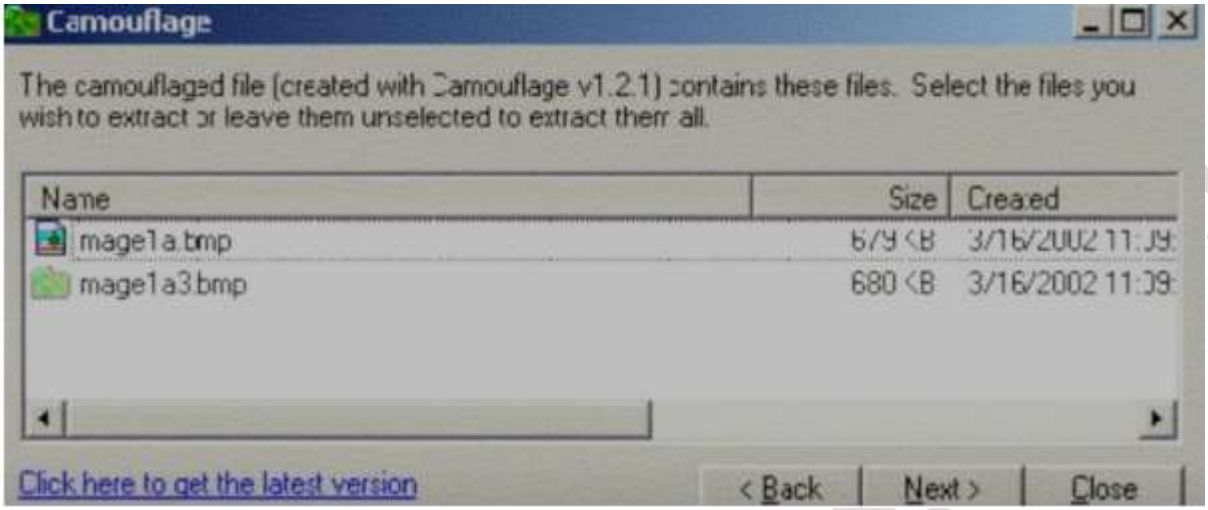
4) A stored password on the file is optional but must be used to open file if it was created when making the file . the ability to add a password toa camouflaged will create a lot of work foe someone that does not have the camouflage program has forgotten . Down is the password dialogue box presented when finalizing a camouflaged file .



To Complete the camouflage process , simply select the finish and a new file is created .The file will behave like a file chosen during the camouflage process and will bear no resemblance to the camouflaged file. The entire camouflage process takes no longer one minute . The resultant image or text file do not have any visible difference than the real one .

UNCAMOUFLAGING FILES

Uncamouflaging the file is a one step process. To uncamouflage a file simply right click the file and select uncamouflage . When selecting Uncamouflage if the file was given a password , after this the password would need to be re-entered .



Steganography has become simple .This ability can be beneficial but can be dangerous too. The ability like simply look at the file and see that it has a hidden message is beyond the capability of human eye .

Camouflage is a software with which the tasks can be completed in an easy way. It is a good program that leaves a trail of the signature which a person can detect easily who will be doing detection of steganography on a file. As there has been so many times that steganography has been used for illegal purposes .So, the solution for this is that multiple items should be addressed such as a person should have complete knowledge about the task that one is accomplishing, about access of steganography and how to implement steganography .If one is going to detect , he/she should consider the key changes which will be a great help for detection. For example : changes such as increase in file size, changes in system settings and many more are indications .Thus, these techniques can be used and implemented by the person who has quite good knowledge of these techniques .

Summary:

When a hidden message is tucked away inside of an ordinary message, this is called steganography. Using this method, you may send a secret message to another individual and ensure that no one else in the chain of command will be privy to it. Real-life communications have employed this technique for a long time.

It has also been employed in digital chats since the emergence of digital communication. The hidden message is inserted into the unused or redundant data of a standard computer file. Images, plaintext, and encrypted messages can all be used to conceal this information. Images, video, and audio files may all be used to conceal plaintext or image messages, among other types of data. It is now possible to use specialised tools for this purpose. Steganography is mostly used to conceal a secret message within a regular file. You will not have to worry about anyone finding out about the file, and your message will remain safe. There will be no problems with the file that was utilised to cloak the message.

It is critical that files are transmitted in a secure manner. Hackers may be found all over the place, and they are constantly on the lookout for new ways to gain access to sensitive information. We can limit the risk of data leaking by utilising steganography. Even if a hacker gains access to your account or email, he will be unable to find the private file you are trying to send. Steganography may be performed in a variety of methods in digital communication.

However, this does not need code. Steganography software is accessible in a variety of forms. Your secret message may be hidden behind any type of file, whether it is an image, HTML, DOC, or any other. It is possible to use steganography in a variety of applications. There are some stenographers who just use steganography, while there are others who encrypt data before hiding it.

There are some that can just conceal data in the image, but others that can hide data in whatever file they choose. Make use of these tools and see what they can do. If you are looking for security in your everyday conversations, I am confident that one of these options will be able to help. Steganography is a feature offered by a wide range of software.

Reference:

- https://en.wikipedia.org/wiki/Steganography_tools
- https://resources.infosecinstitute.com/topic/steganography-and-tools-to-perform-steganography/
- https://embeddedsw.net/OpenPuff_download.html