INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

“Steganography”

By:

Manzano Salazar Leonardo

Moreno Zarate Victor Gibran

Professor:
M. en C. NIDIA ASUNCIÓN CORTEZ DUARTE

16th December 2016

Index

Contenido

Problem:

If I want to hide a message in an image… How Will I do?

STEGANOGRAPHY

Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication-to hide the existence of a message from a third party. This paper is intended as a high-level technical introduction to steganography for those unfamiliar with the field. It is directed at forensic computer examiners who need a practical understanding of steganography without delving into the mathematics, although references are provided to some of the ongoing research for the person who needs or wants additional detail. Although this paper provides a historical context for steganography, the emphasis is on digital applications, focusing on hiding information in online image or audio files. Examples of software tools that employ steganography to hide data inside of other files as well as software to detect such hidden files will also be presented.

In modern digital steganography, data is first encrypted by the usual means and then inserted, using a special algorithm, into redundant (that is, provided but unneeded) data that is part of a particular file format such as a JPEG image. Think of all the bits that represent the same color pixels repeated in a row. By applying the encrypted data to this redundant data in some random or nonconspicuous way, the result will be data that appears to have the "noise" patterns of regular, nonencrypted data. A trademark or other identifying symbol hidden in software code is sometimes known as a watermark[1].

Hypothesis:

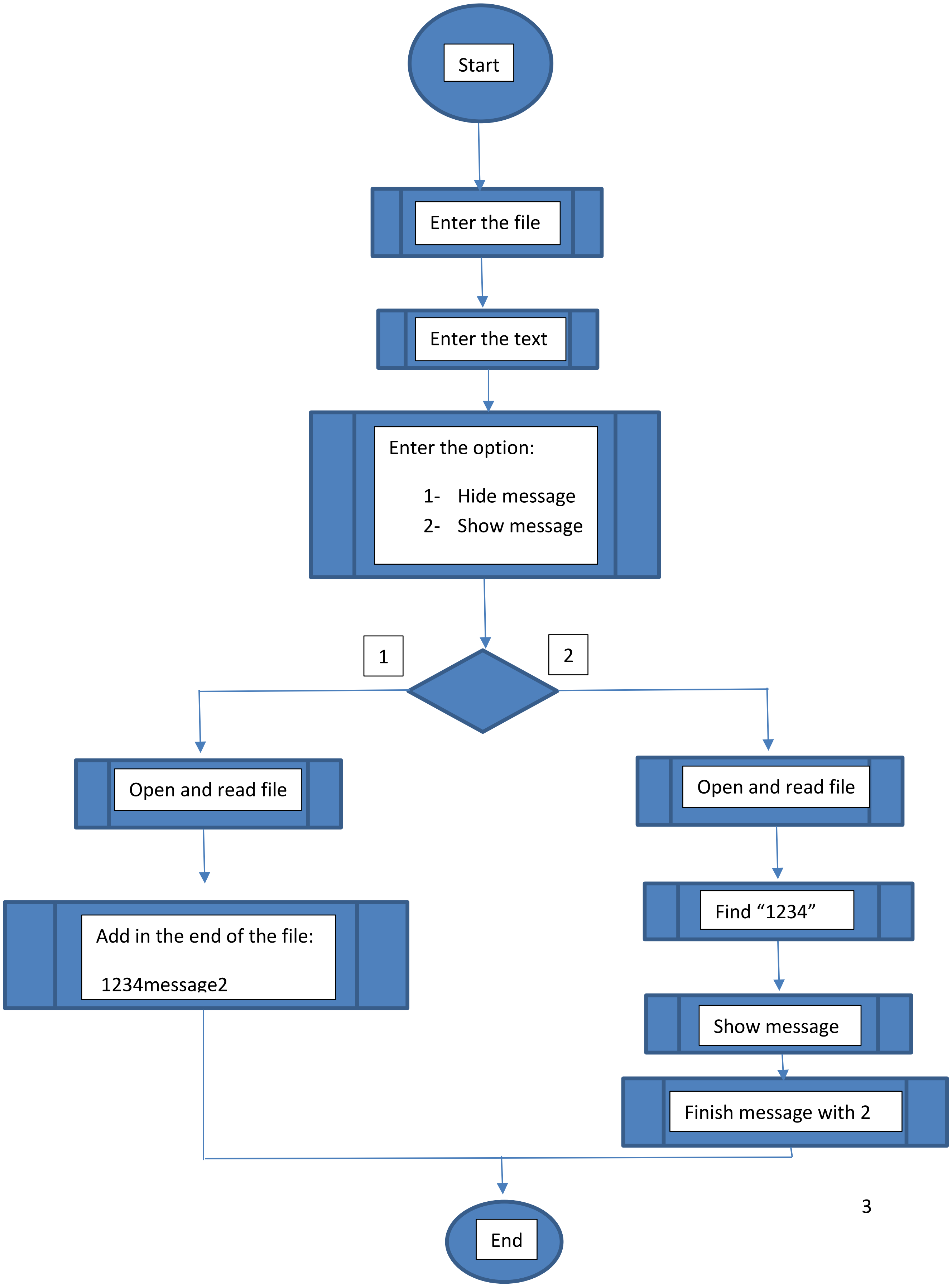
We have to find an algorithm that hide a message in an image with JPG format. A possible solution is adding in the end of file the text.

Software (libraries, packages, tools):

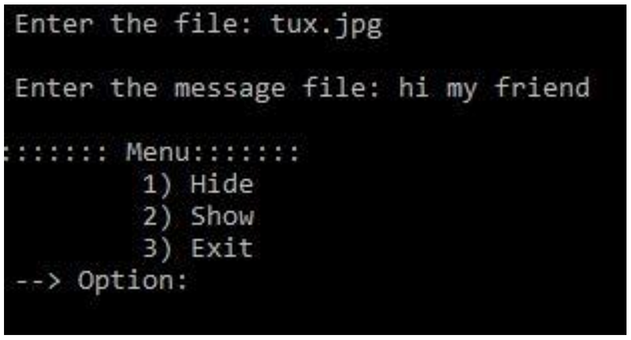
We use:

- Linux Operating System
- GCC compiler
- Personal Computer

Procedure:


Start
Enter the file
Enter the text
Enter the option:
1- Hide message
2- Show message
1
2
Open and read file
Add in the end of the file:
1234message2
Open and read file
Find “1234”
Show message
Finish message with 2
End

Results (Data):

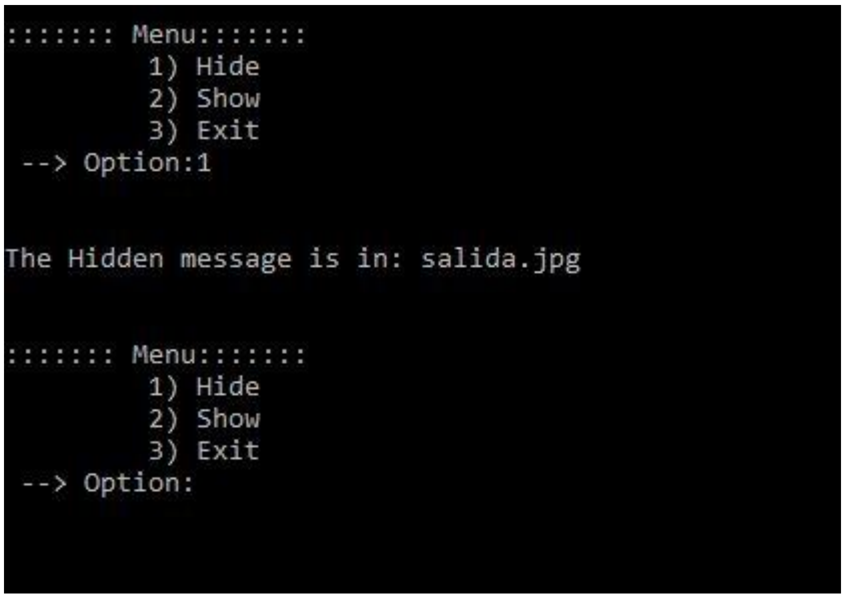


```
Enter the file: tux.jpg

Enter the message file: hi my friend

:::::: Menu:::::::
        1) Hide
        2) Show
        3) Exit
--> Option:
```

Figure1: Enter the file and the message

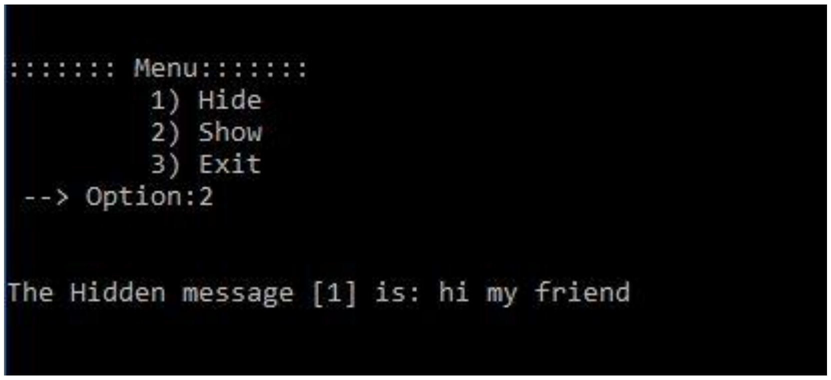


```
::::::: Menu:::::::
         1) Hide
         2) Show
         3) Exit
 --> Option:1


The Hidden message is in: salida.jpg


::::::: Menu:::::::
         1) Hide
         2) Show
         3) Exit
 --> Option:
```

Figure2: The message hides


```
::::::: Menu:::::::
        1) Hide
        2) Show
        3) Exit
 --> Option:2


The Hidden message [1] is: hi my friend
```

Figure3: The message is “hi my friend”

Conclusions:

In this practice, we can hide a message in an jpg image and show the original message, we use a simple algorithm that add in the end of file the text, in this example the text was “hi my friend”.

References:

[1] http://www.garykessler.net/library/fsc_stego.html

Code

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

int main(){

    int opcion;
    char source[30];
    char decrypt[30];
    char message[80];

    FILE *fichero, *destino;
    unsigned char c;
    printf("\n Enter the file: ");
    fgets(source, 30, stdin );
    strtok(source, "\n");
    /*printf("\n Enter the message: ");
    fscanf(stdin, "%s", message);*/
    printf("\n Enter the message file: ");
```

```c
    fgets(message, 30, stdin );
    strtok(message, "\n");
    do{

            printf("\n::::::: Menu:::::::");
            printf("\n\t 1) Encrypt");
            printf("\n\t 2) Decrypt");
            printf("\n\t 3) Exit");
            printf("\n --> Option:");
            fflush(stdin);

            scanf(" %d",&opcion);
            if(opcion==1)
            {
                destino=fopen("salida.jpg","ab");
                fichero= fopen(source, "rb");

                while(1)
                {
                        c = fgetc(fichero);
                        if(!feof(fichero))
                        {
                             fputc(c,destino);

                        }
                        else
                            break;


                }

                fclose(fichero);

                fwrite( "1337", strlen("1337"), 1, destino );

                fwrite( message, strlen(message), 1, destino );

                c=2;

                fwrite( &c, 1, 1, destino );

                fclose(destino);

                printf("\n\nThe Hidden message is in: salida.jpg \n\n" );


            }

            else if(opcion==2)
            {
                unsigned char *buffer;
                int conta, d, i, mensajes;
                fichero= fopen("salida.jpg", "rb+");
                if(fichero != NULL)
                {

                   while(fread( &d, 1, 1, fichero ) > 0)
                          conta++;

                    if((buffer=malloc(conta))!=NULL)
                    {
```

```c

                 rewind(fichero);

                 fread(buffer, conta, 1, fichero);


                 for(i=0, mensajes=0; i+3<conta ; i++)
                 {


                   if(buffer[i]=='1' && buffer[i+1]=='3' && buffer[i+2]=='3' && buffer[i+3]=='7')
                   {

                     printf("\n\nThe Hidden message [%d] is: ", mensajes+1);


                     i+=4;

                     while(buffer[i]!=2)
                                 putchar(buffer[i++]);

                            mensajes++;

                            printf("\n\n");

                          }


                        }

                        free(buffer);

                    }
                    else
                        printf("\n\nERROR: RAM isn't enough\n\n");

                    fclose(fichero);

                    if(!mensajes)
                        printf("\n\nThe file doesn't have Hidden messages\n\n");

                }



            }
    }while(opcion==1 || opcion==2);

    return 0;
}
```