CSE4019 – IMAGE PROCESSING

LSB STEGANOGRAPHY – MESSAGE ENCRYPTION IN IMAGES

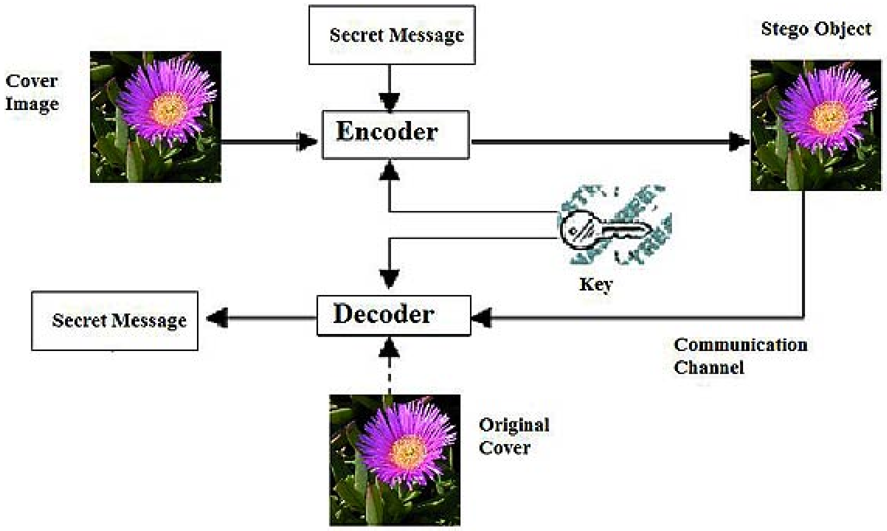
IMPLEMENTED BY:
ADITYA RAMESH – 16BCE0948

UNDER THE GUIDANCE OF:
PROF. AKILA VICTOR

INDEX

ABSTRACT

Steganography is the technique of encrypting data in a data carrier (an image, in this case) in such a manner that it is impossible for an outsider to identify that a message has been encrypted into the image. The data carrier may also be an audio file or a text file, however an image file has been considered for the following. This technique is different from other data hiding methods like watermarking, in the way that it is far more subtle. The watermark's presence is often broadcasted entirely over the image, which prevents any communication/message to be secretive or discreet.

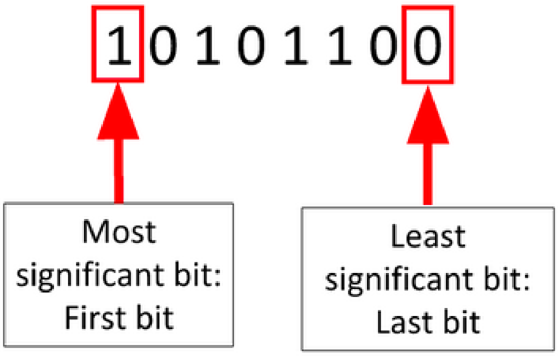


OBJECTIVE

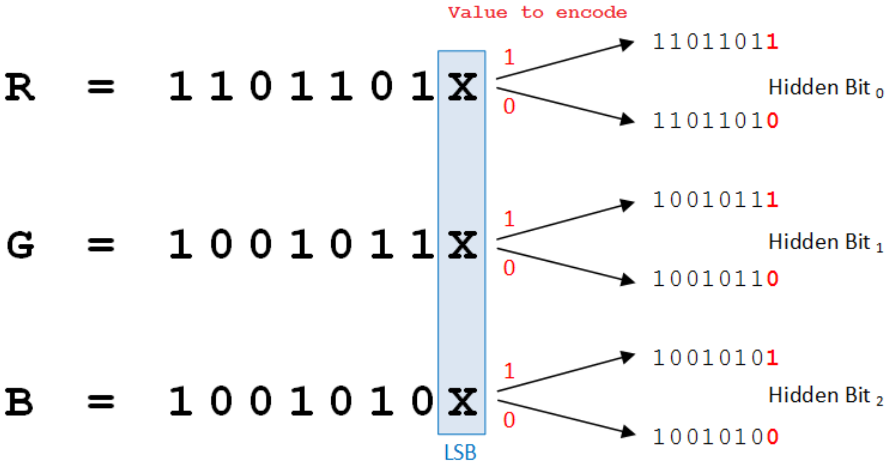
The objective of this project is to attempt to successfully, discreetly encrypt a text message into an image file, and also decrypt the same text from the encrypted file. The implementation overwrote the image file's bits based on the secret message's bits.

METHODOLOGY

Image steganography is the most popular form of its kind, and consists of two components – the cover image and the secret file. This secret file could be text or audio or image. This is the data that must be encrypted into the cover image. The bits of this secret file are embedded in the bits of the cover image by modifying the content of the least significant bit, in the case of the LSB Algorithm.


1 0 1 0 1 1 0 0
Most significant bit: First bit
Least significant bit: Last bit

In the Lowest Significant Bit algorithm, **the information is hidden in the last bits of the pixels in the cover image.** The LSB is the least significant bit in the byte value of a pixel in the image. In a 24-bit image, the three basic colors present that contribute to 24 bytes (8 + 8 + 8) are Red, Green and Blue. Each represents 1 byte. An 800 x 600 image can store 1440000 bits of encrypted information consequently. A change in the LSB of a pixel is evidenced by minor changes in the intensity of the colors. These changes are usually too little to be detected by the naked eye, and thus the steganogramme is generated.



LIMITATIONS

The primary issue however is that the LSB method limits the size of data that can be encrypted to about 1/8th of the size of the cover image, as each pixel can only store one bit of encrypted information in its last bit, and consequently, the larger the message to be encrypted, either the cover image must be larger, or more number of bits must be used from the cover image to hide more in lesser space.

However the problem with using more number of bits to store the encrypted image/message in the cover image, is that as the number of bits used to store the encrypted message increases, the likelihood of the image being morphed and modified being detected also increases, consequently lowering its subtlety. Thus, this is the largest limitation of this algorithm.

APPLICATIONS

Yet, its applications are many, and the algorithm is found to be used in the following -

- Secret data storing and communication
- Media database systems
- Access control systems for digital content distribution and marketing

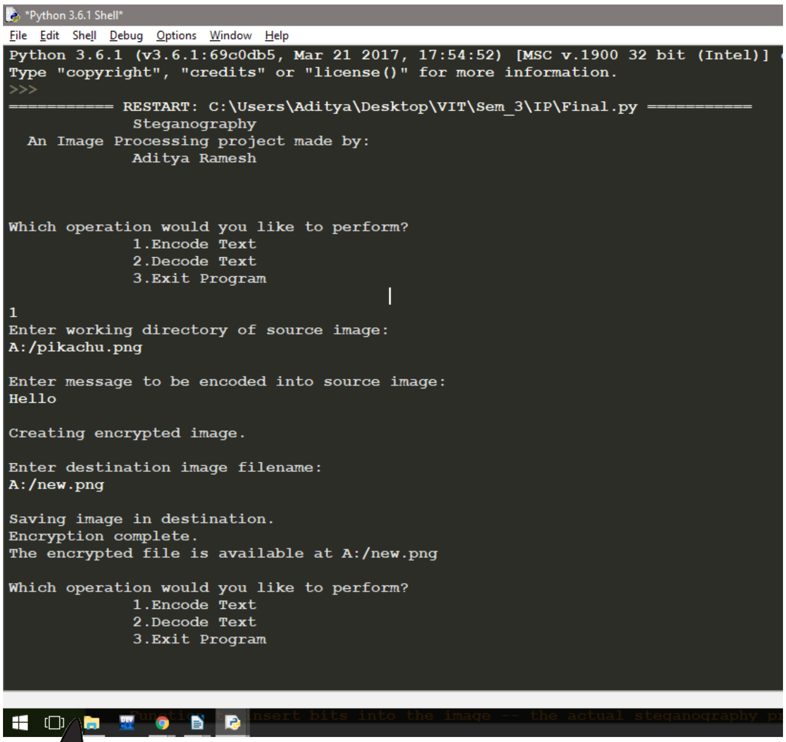
The potential of steganography is evident at hiding the existence of confidential data, the difficulty there exists in detecting the presence of hidden data, and the enhancement in security due to the increase in difficulty of decrypting the encrypted data.

Steganography is also used in modern printers, wherein brand color laster printers add small yellow dots to each page. These dots encode printer serial numbers and date-and-time stamps for traceability and additional information.

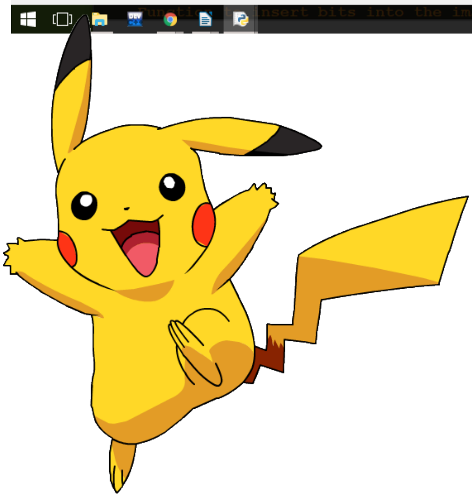
Steganography is also used in digital watermarking messages, acting as identifiers, by hiding in images and allowing images to be tracked and verified.

Reports from the Federal Bureau of Investigation also claim that the Russian Foreign Intelligence service use customized steganography software to encrypt text messages inside cover images for discreet communication with agents stationed abroad.

SCREENSHOTS



```
Python 3.6.1 (v3.6.1:69c0db5, Mar 21 2017, 17:54:52) [MSC v.1900 32 bit (Intel)]
Type "copyright", "credits" or "license()" for more information.
>>>
=========== RESTART: C:\Users\Aditya\Desktop\VIT\Sem_3\IP\Final.py ===========
             Steganography
  An Image Processing project made by:
             Aditya Ramesh



Which operation would you like to perform?
             1.Encode Text
             2.Decode Text
             3.Exit Program

1
Enter working directory of source image:
A:/pikachu.png

Enter message to be encoded into source image:
Hello

Creating encrypted image.

Enter destination image filename:
A:/new.png

Saving image in destination.
Encryption complete.
The encrypted file is available at A:/new.png

Which operation would you like to perform?
             1.Encode Text
             2.Decode Text
             3.Exit Program
```



Original Image – pikachu.png(23 KB)

Encrypted Image – new.png (47 KB)

IMPLEMENTATION

The implementation of this project is available at: github.com/rameshaditya/steganography

RESULTS

Thus, LSB text-based steganography has successfully been implemented

FUTURE SCOPE

The above implementation only implements text encryption however image encryption and potentially audio encryption are also feasible possibilities provided the size of the message is lesser than the one-eighth the size of the image.

REFERENCES

Wendzel, Steffen; Mazurczyk, Wojciech; Haas, Georg. "Information Hiding In Cyber Physical Systems Using Smart Buildings". *Proceedings of the 2017 IEEE Security & Privacy Workshops*. IEEE.

Krzysztof Szczypiorski (4 November 2003). "Steganography in TCP/IP Networks. State of the Art and a Proposal of a New System – HICCUPS". *Institute of Telecommunications Seminar*. Retrieved 17 June 2010

Mazurczyk, Wojciech; Wendzel, Steffen; Zander, Sebastian; Houmansadr, Amir; Szczypiorski, Krzysztof (1 February 2016). *Information Hiding in Communication Networks: Fundamentals, Mechanisms, and Applications*(1 ed.). Wiley-IEEE. ISBN 978-1-118-86169-1.

"Secret Code in Color Printers Lets Government Track You; Tiny Dots Show Where and When You Made Your Print". Electronic Frontier Foundation. 16 October 2005.

"Criminal complaint by Special Agent Ricci against alleged Russian agents" . United States Department of Justice.