DEPSTAR

CHARUSAT
CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY

Steganography in Images

GUIDED BY: VIDHI PANDYA
ATUFA SAIYED

18DCS045 RUTIKA MEHTA
18DCS067 DHRUV PATEL

Introduction

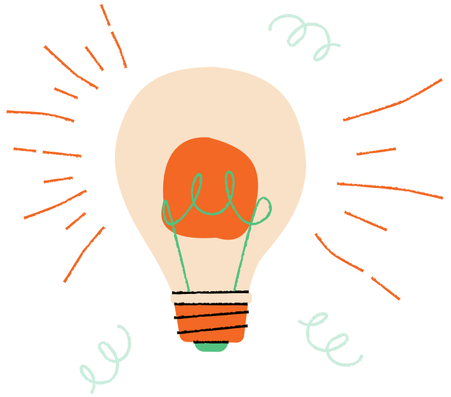
Steganography comes from a greek word.

Stegan-o-grapy

Covered

Writing

Think about it!



-> The goal of steganography is to hide messages in such a way that no one apart from the intended recipient even knows that a message has been sent.

-> This can be achieved by concealing the existence of information within seemingly harmless carriers or cover

Steganography in Images

Image Compression:

- Image compression offers a solution to large image files. Two kinds of image compression are lossless and lossy compression. Both methods save storage space but have differing effects on any uncompressed hidden data in the image.

- “Lossy” JPEG(Joint Photographic Experts Group) format files, offers high compression, but may not maintain the original image's integrity. Hence it is called “lossy”.

- “Lossless” compression maintains the original image data exactly, It is thus more favored by steganographic techniques. Eg: (BMP),(GIF) Formats.

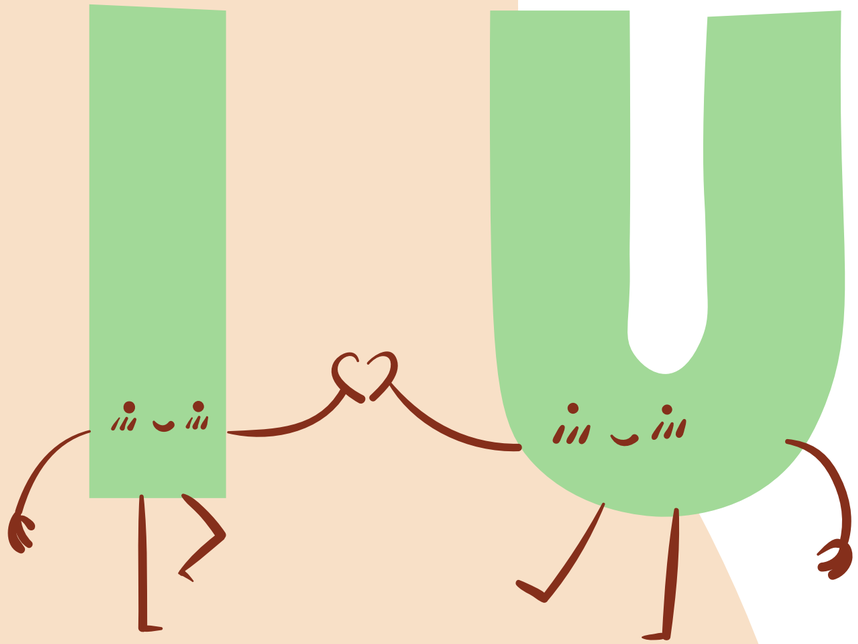
Features we're gonna provide

- **Perceptual Transparency:** Each cover-media has certain information hiding capacity. If more information or data is hidden inside the cover, then it results in degradation of the cover–media. As a result, the stego–media and cover–media will appear to be different.

- **Robustness:** Robustness is the ability of the hidden message to remain undamaged.

- **Tamper–resistance:** If the attacker is successful in destroying the steganographic technique then the tamper–resistance property makes it difficult for the attacker or pirates to alter or damage the original data.

Working of the Application



The method used for system is the Least Significant Bit (LSB) method in which the secret information is hidden in the least significant bits of the image.
There are 2 different LSB steganographic methods: LSB Replacement and LSB Matching. This system uses LSB Replacement, in which we change the least significant bit with one bit of the secret message which we want to hide.

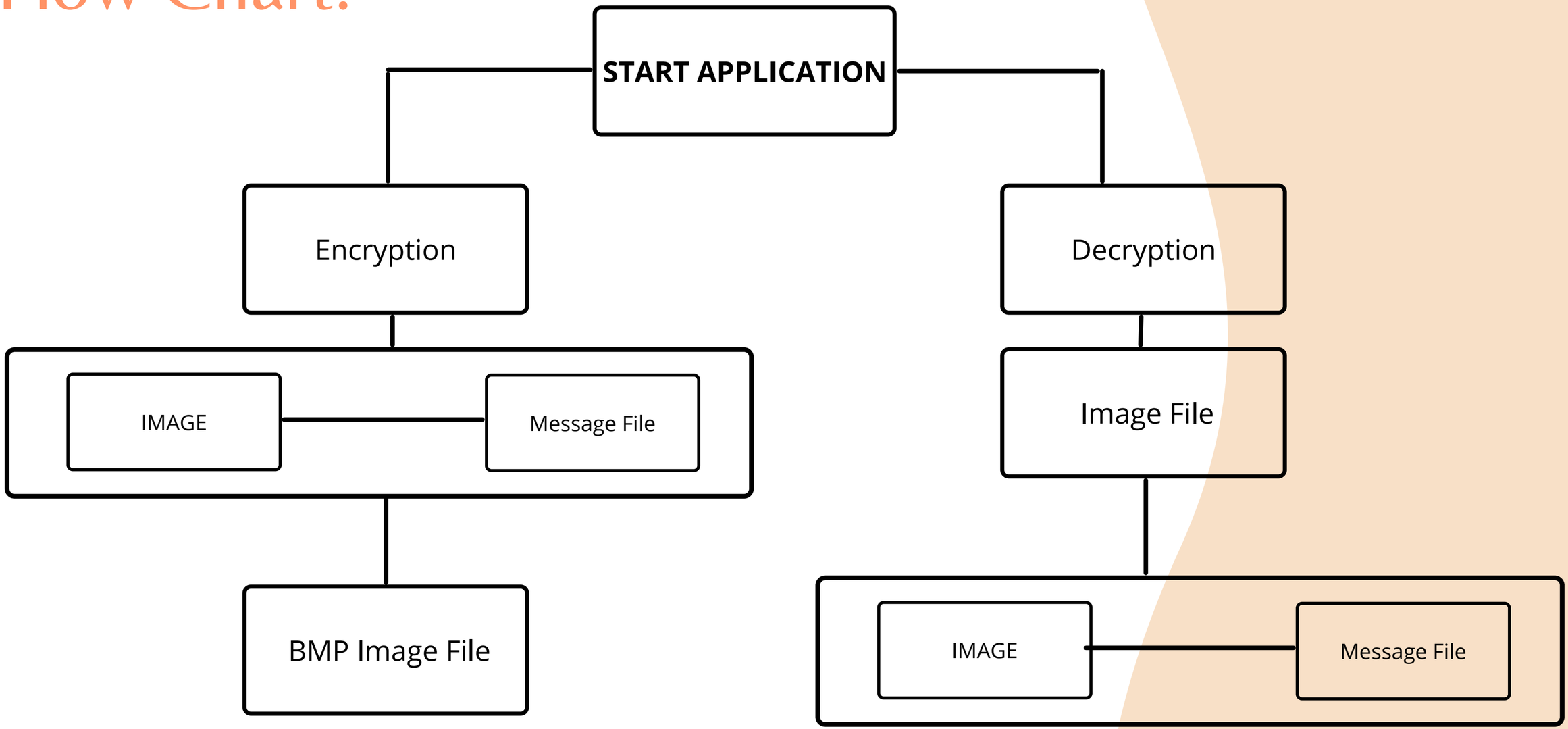
Encode the data:

Every byte of data is converted to its 8-bit binary code using ASCII values. Now pixels are read from left to right in a group of 3 containing a total of 9 values. The first 8-values are used to store binary data. The value is made odd if 1 occurs and even if 0 occurs.

Decode the data:

To decode, three pixels are read at a time, till the last value is odd, which means the message is over. Every 3-pixels contain a binary data, which can be extracted by the same encoding logic. If the value if odd the binary bit is 1 else 0.

Flow Chart:


START APPLICATION
Encryption
Decryption
IMAGE
Message File
Image File
BMP Image File
IMAGE
Message File

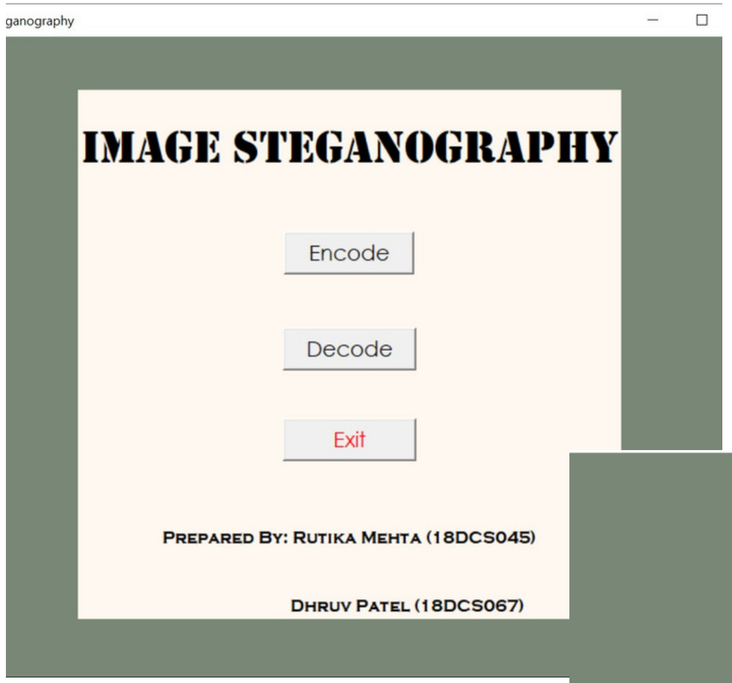
Future Scope

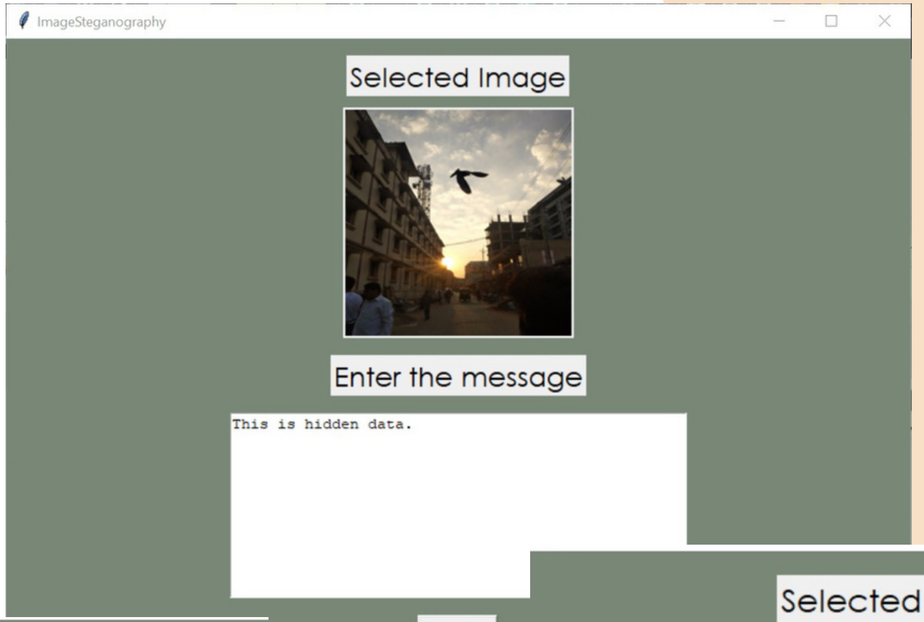
Voice over Internet Protocol (VoIP) used for steganography owing to its difficulty in detecting hidden information in VoIP streams.

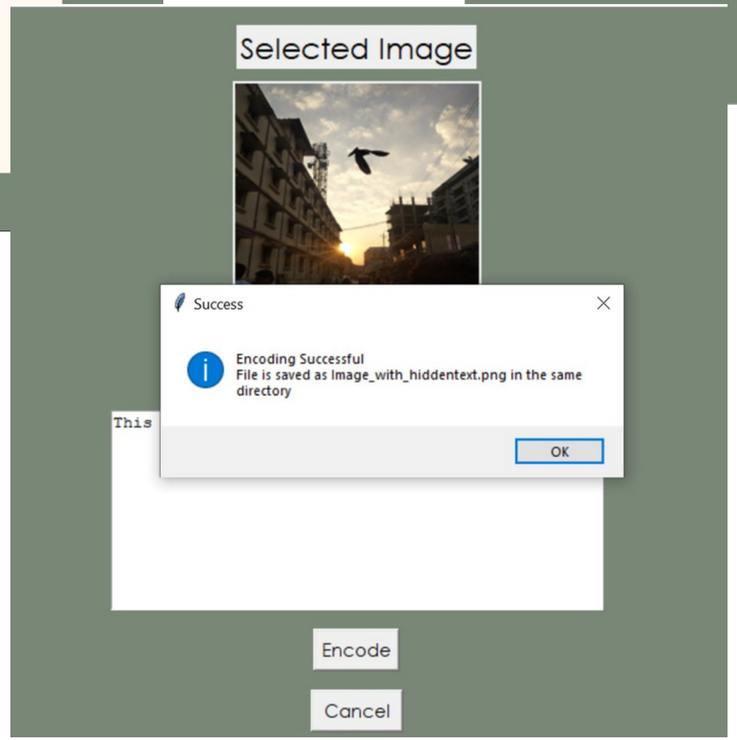
Steganography is capable of mitigating piracy by aiding copyright marking.

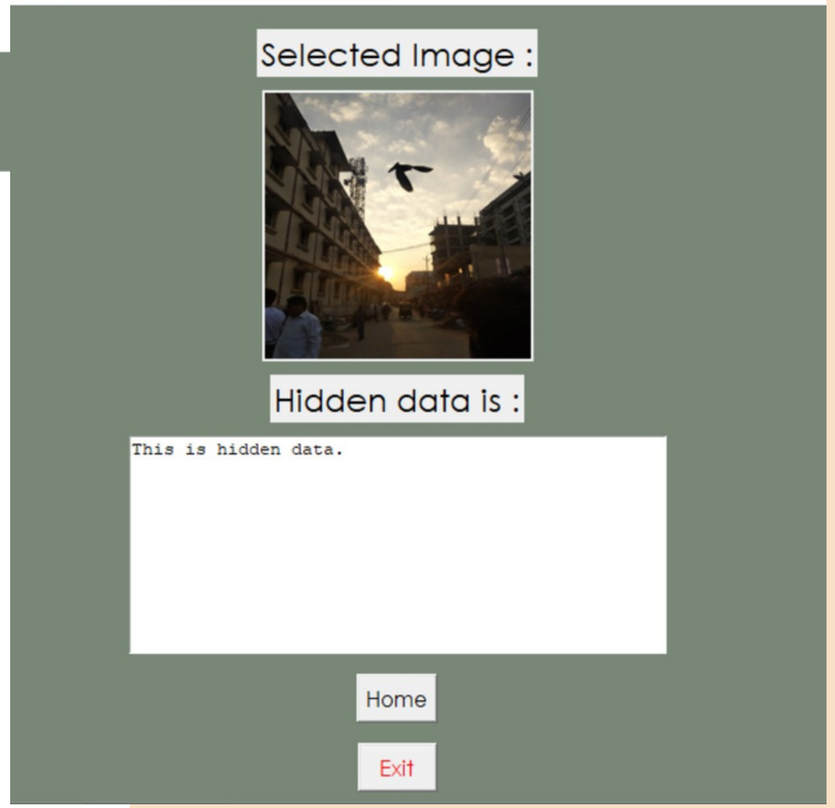
Digital camera manufacturers could implement steganographic features as a part of camera firmware to annotate pictures with the photographer's copyright information.

Screenshots









References

>https://towardsdatascience.com/steganography-hiding-an-image-inside-another-77ca66b2acb1

> https://www.edureka.co/blog/steganography-tutorial

>https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#191d0b0160ba

>https://www.ukessays.com/essays/computer-science/steganography-uses-methods-tools-3250.php

>https://www.thepythoncode.com/article/hide-secret-data-in-images-using-steganography-python

> https://www.youtube.com/watch?v=xepNoHgNj0w&t=1922s

>https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/steganography-what-is-that/