AHMEDABAD UNIVERSITY

Global Education at Local Cost, Context and Ethos™

Steganoid

A Tool for Image – Audio Steganography

Himanshu Moliya

Outline

- Overview
- Seven Phase of this Application
- System Model
- Features
- Core concept
- User interface
- Implementation
- Future Scope

Overview : Steganography

- The word steganography comes from the Greek name “steganos” (hidden or secret) and “graphy” (writing or drawing) and literally means hidden writing.

- **Steganography uses techniques to communicate information in a way that is hidden**.
- Steganography hides the existence of a message by transmitting information through various carriers. Its goal is to prevent the detection of a secret message.
- The most common use of steganography is hiding information from one file within the information of another file.

Cover medium + Hidden information + Stegokey = Stego-medium

Two layer of security

- This application provides two level of security.

1. Steganography
2. AES encryption

Why this?

- This two layer provide high level of security to prevent attack on stegano image and stegano audio.

Seven Phase of this Application

1. **Image Steganography :** User can hide any file inside the image. It may be Cipher file / Text file Image file, PDF file,… etc.

2. **Audio Steganography :** User can hide cipher data inside the audio.

3. **AES Encryption :** This application use advanced Encryption standards internally.

Seven Phase of this Application

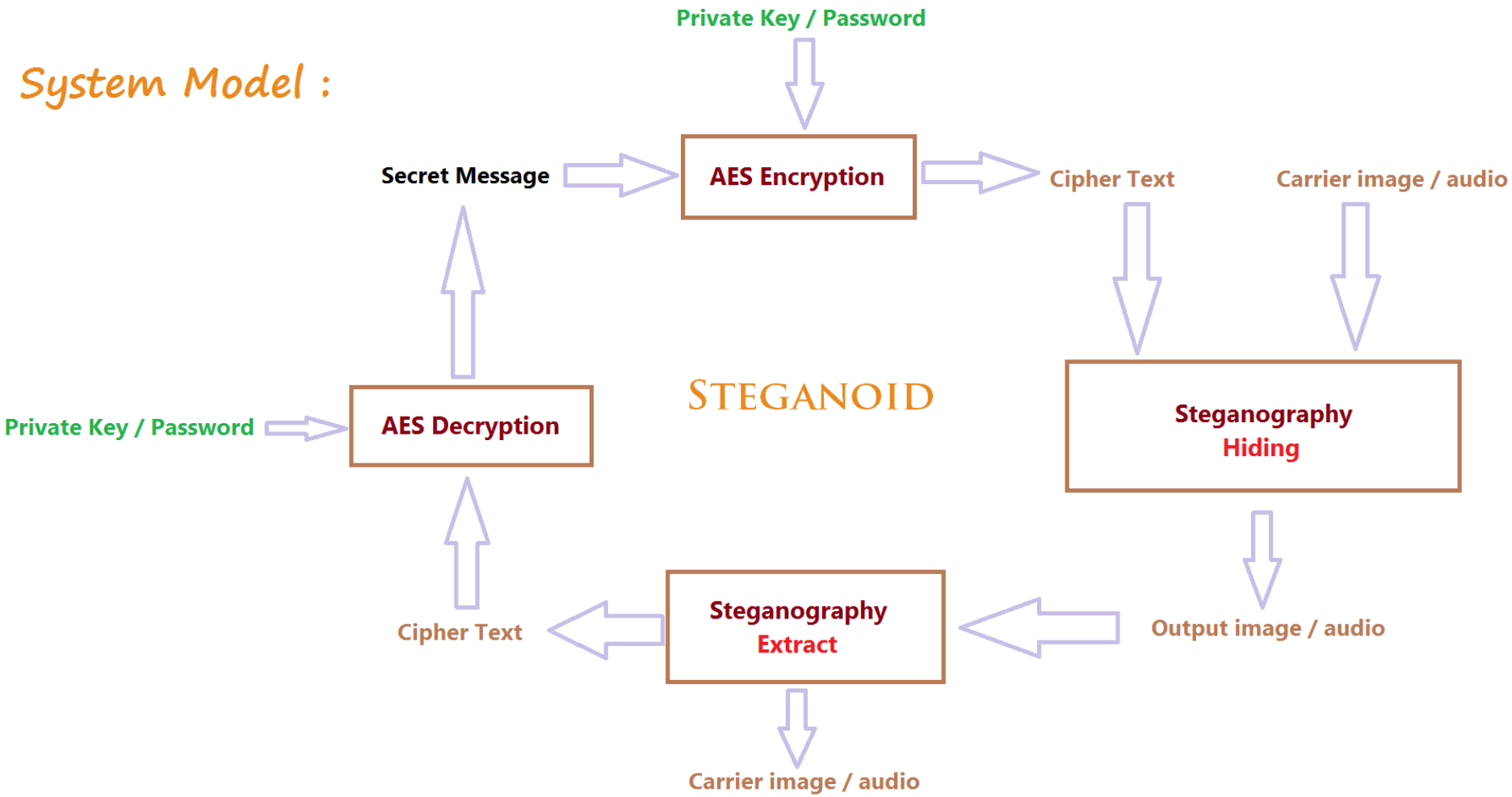
4. Change format: Data must be consistent after change format of image (e.g. : BMP to PNG)

5. Data minimization: Store data with in same size image.

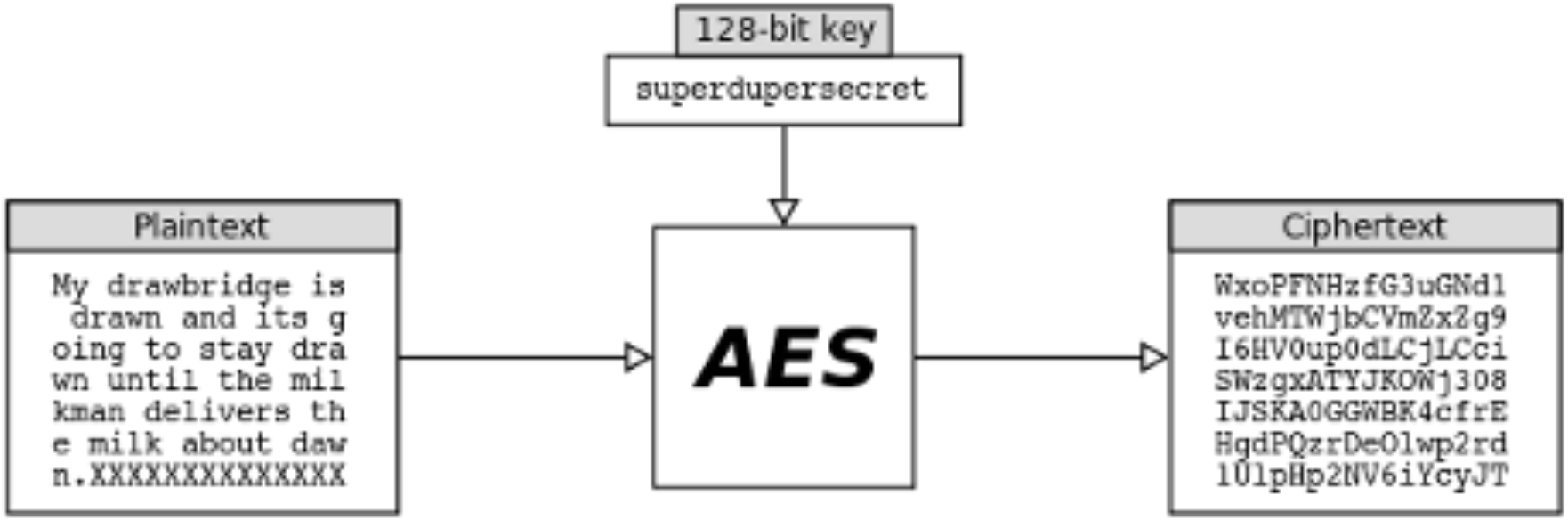
6. Attack testing: AES encryption provide security to prevent visual attack.

7. Digital water marking: This application also use as Digital water marking application.

System Model :



AES Encryption :



Reference: http://www.lightwaveonline.com/articles/2016/01/the-evolution-and-implementation-of-encryption-across-layer-1-networks.html

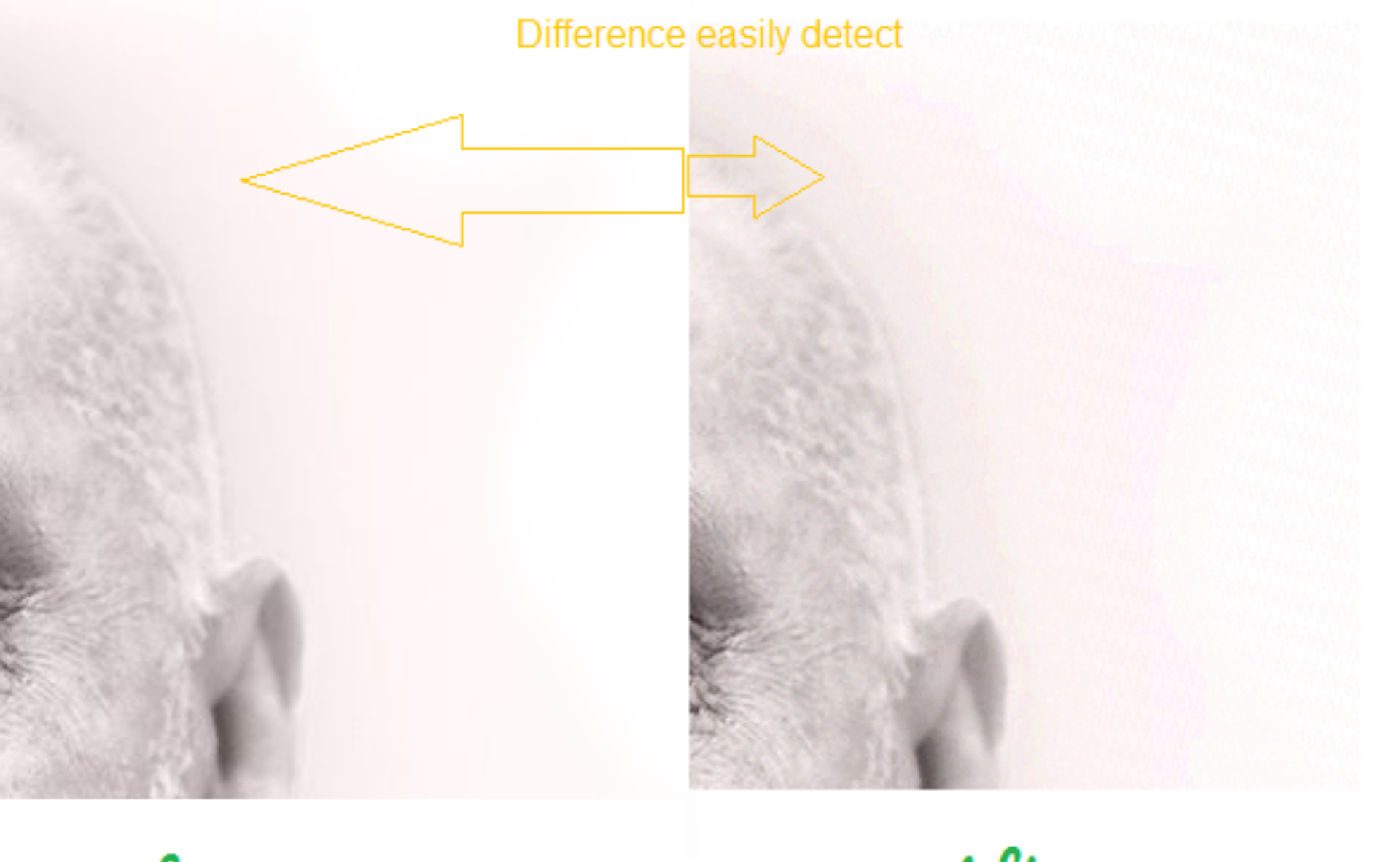
Features : Steganoid

1. Image Steganography
2. Audio Steganography
3. Use AES Encryption (Advanced Encryption Standard)
4. Use Symmetric Cryptography / Symmetric key use
5. Data consistently after changing format
6. Data Minimization
7. Test attack : safe data in visual attack
8. Use as Digital water marking Tool.

Security over visual Attack

What is visual attack?

Visual Attacks are simplest form of steganalysis that involves examining the stego-image with the naked eye to identify any kind of degradation.


Difference easily detect
Before Hiding
After Hiding

Security over visual Attack

- This application also provide security against visual attack.

How ?

- If someone detect text from the image and extract it from the image.
- They can’t read it because of encrypted text (Need to break AES algorithm to read that data)(i.e very difficult)

Core concept Implementation

Encoding Schema (LSB) : Image

One character (in Integer form)

Pixel value

```
7 references
public static Color EncodePixel(Color pixel, int value)
{
    //Encoding Style.
    int blueValue = value & 7;//& with 0000 0111 (last three bit save in blue pixel)
    int greenValue = (value >> 3) & 7;//& with 0011 1000 (three bit save in  green pixel)
    int redValue = (value >> 6) & 3; // & with 1100 0000 (first two bit save in rad pixel)

    int red = (pixel.R & 0xFC) | redValue; //0xFC=11111100
    int green = (pixel.G & 0xF8) | greenValue;//0xF8=11111000
    int blue = (pixel.B & 0xF8) | blueValue;

    return Color.FromArgb(red, green, blue);// Generate new pixel and return
}
```

Generate New pixel

Generate new RGB

Data hide in RGB Channel

Decoding Schema (LSB) : Image

Reverse process of encoding : decode text from each pixel.

```
4 references
public static int DecodePixel(Color pixel)
{
    //decoding Style : similer as encoding
    int red = (pixel.R & 3);
    int green = (pixel.G & 7);
    int blue = (pixel.B & 7);
    int value = blue | (green << 3) | (red << 6);
    return value;
}
```

Encoding Schema (LSB) : Audio

8 bit for each character / each character take as value

```
myConsole.Write("Processing wav file...");
for (int i = 0; i < encrypted.Length; i++)
{
    value = encrypted[i];
    for (int x = 0; x < 8; x++)
    {
        uint sample = generator.Next;
        uint sampleValue = audio.samples[sample];
        sampleValue = (sampleValue & 0xFFFFFFFE) | ((value >> x) & 1);//One bit per sample
        audio.samples[sample] = sampleValue;
    }
}
```

Pass to new audio sample

Hide one bit in each sample

Decoding Schema (LSB) : Audio

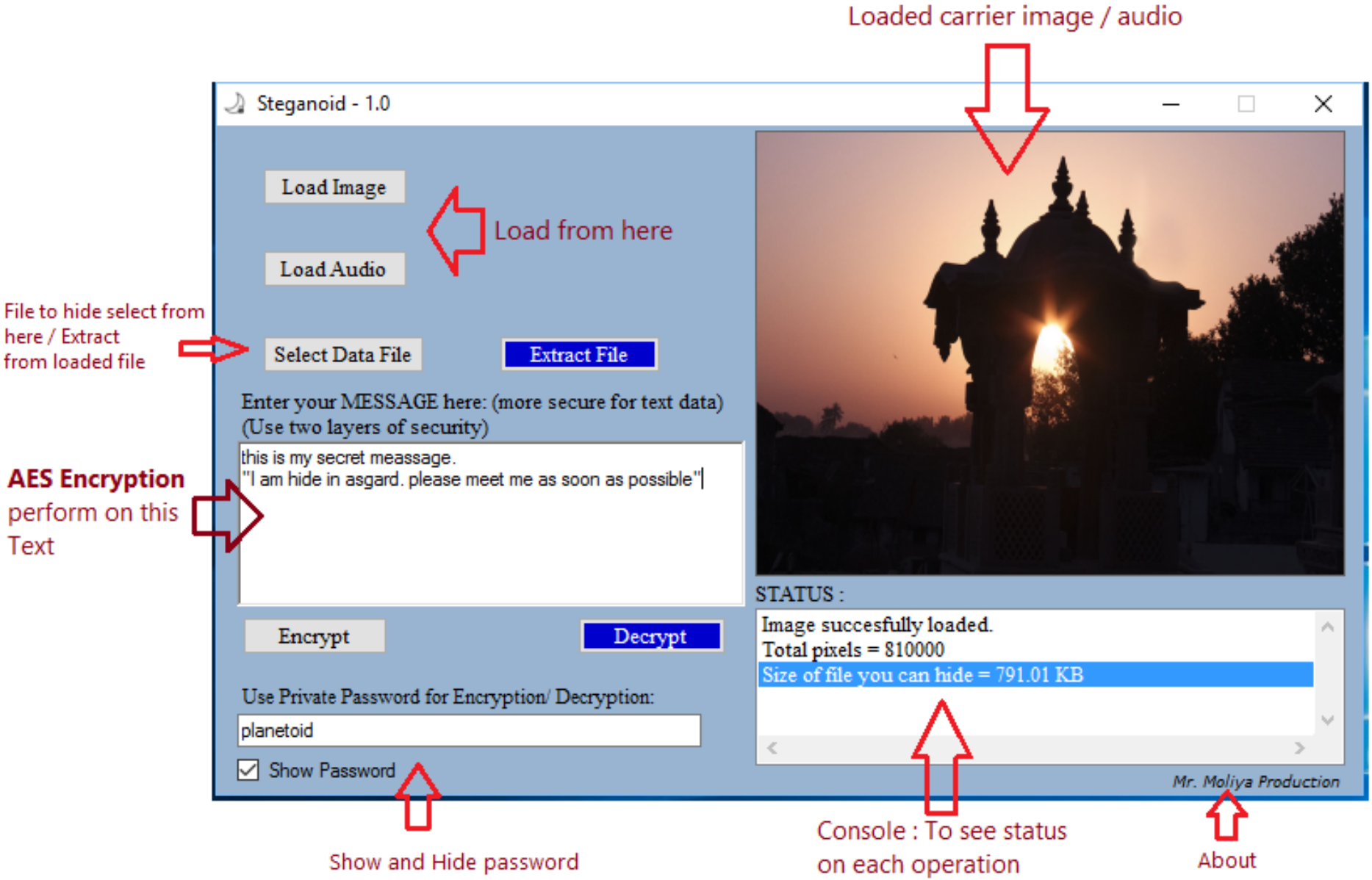
8bit for each character

```
AESAlgorithm encrypt = new AESAlgorithm();
myConsole.Write("Processing wav file...");
do
{
    value = 0;
    for (int x = 0; x < 8; x++)
    {
        uint sample = generator.Next;
        uint sampleValue = audio.samples[sample];
        value = value | ((sampleValue & 1) << x);
    }
    if (value != 0)
        text += Convert.ToChar(value);
} while (value != 0);
```

Generate cipher text from value

Recover value from each sample

User interface :

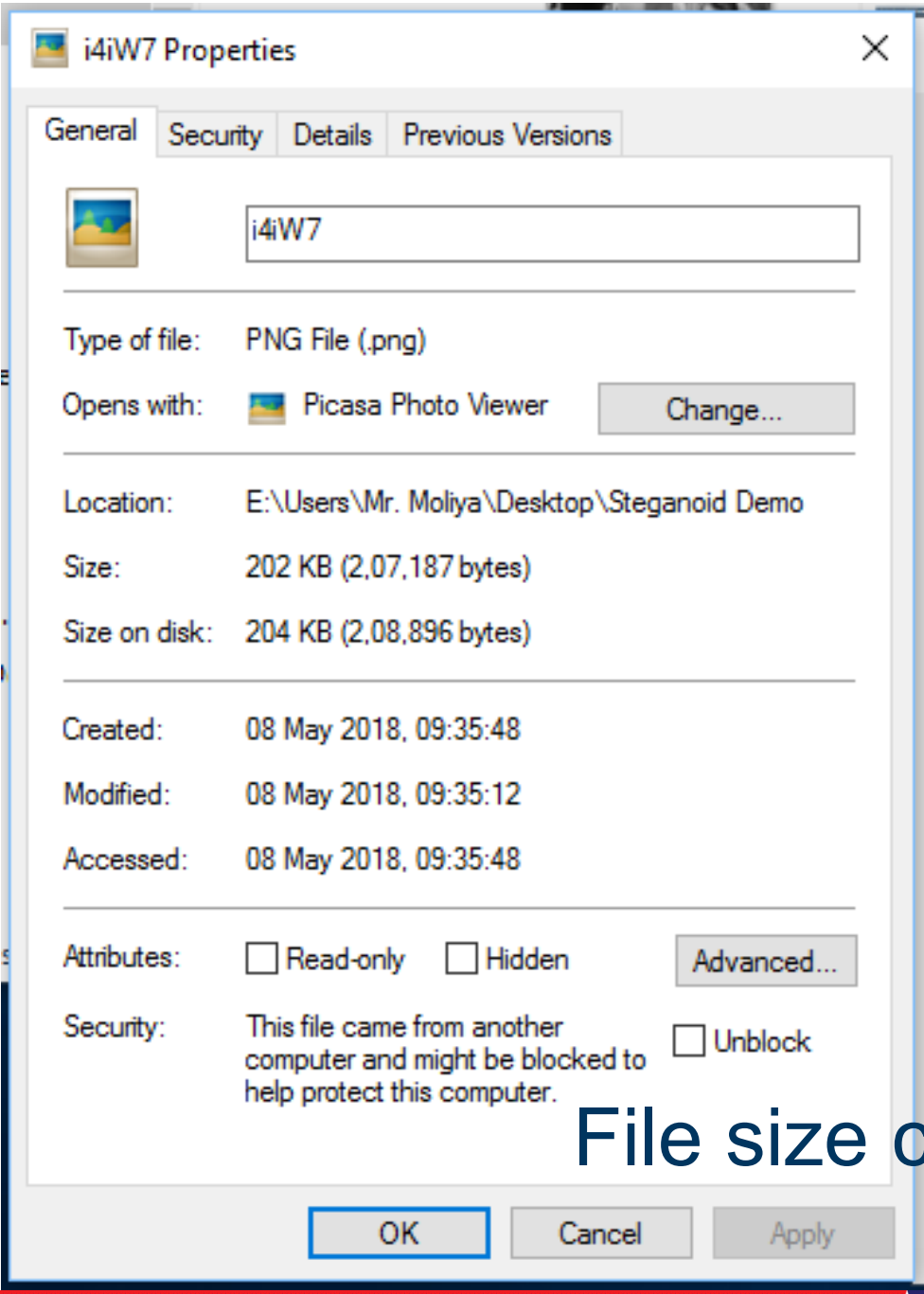


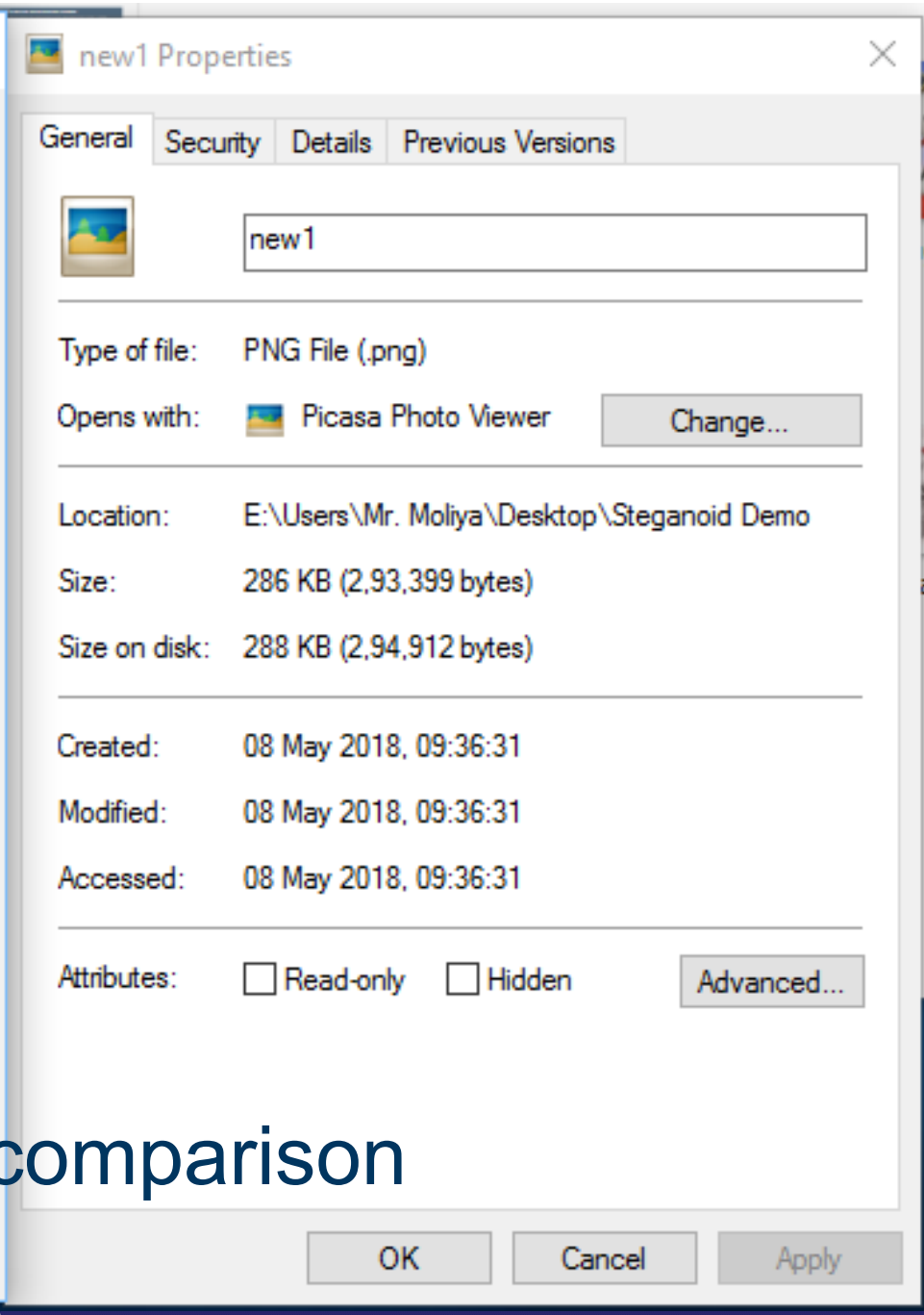
User interface Guidelines :

- Status Console :
  - Provide information **how much data you can hide in that image / audio ?** Also provide details of total pixel / sample**.**
  - Display Cipher text.
  - Display success message, processing message.

- Password :
  - Password for cipher text is used as 2nd layer of security.

  (i.e. can't easily breakup because it used as key for AES algorithm.)
  - Show password button use to see password text for user.





File size comparison

Change format :

Data must be safe after changing file format.

Task:

- I have one Setgo image in BMP format with hidden file ABC.
- now I change format of file to PNG.

Observation :

- Hidden file must be safe after changing format.
- We can easily extract data from PNG file.
- It’s fail in some cases.

(i.e. BMP to JPG or PNG to JPG because of JPG generate compressed image)

Data consistency : after converting to other format

Format	Conversion	Possibility
BMP	BMP	YES
	PNG	
	JPEG	NO (Due to lossy algo)
PNG	BMP	YES
	PNG	
	JPEG	NO (Due to lossy algo)
JPEG	BMP	YES
	PNG	

Data minimization:

Let’s assume we have one user data and it’s contains:

1. 800x600 image with 8bit depth have at most 600 KB size.
2. And all other data (Name, Address, Father name, birthdate(DOB), Finger print data, etc…) Let’s assume this all have 424 KB (size of all Another data)

Now,
Total data of this user = Image + Another data = 600 + 424 = 1024 KB = 1MB.

One user has 1MB data.

But using this model, we can store this **424 KB** taxable data within 600 KB image.

So, we require only 600KB to store one user information (i.e. image size) instead of 1MB.

Concept: After performing Steganography on BMP file **New file size** is same as **Old file size**.

Data minimization:

Now, try to think this model with 125 crore users,

Before:

To store 125 crore user information 125x107 MB required (i.e. 1250 TB).

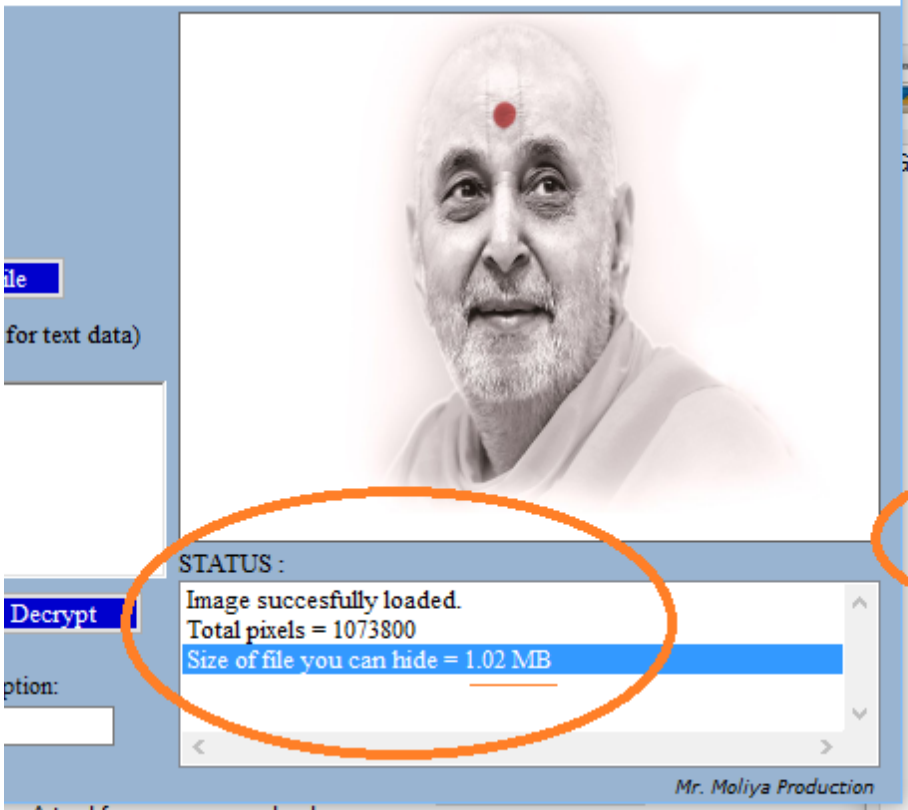
After Applying this model:

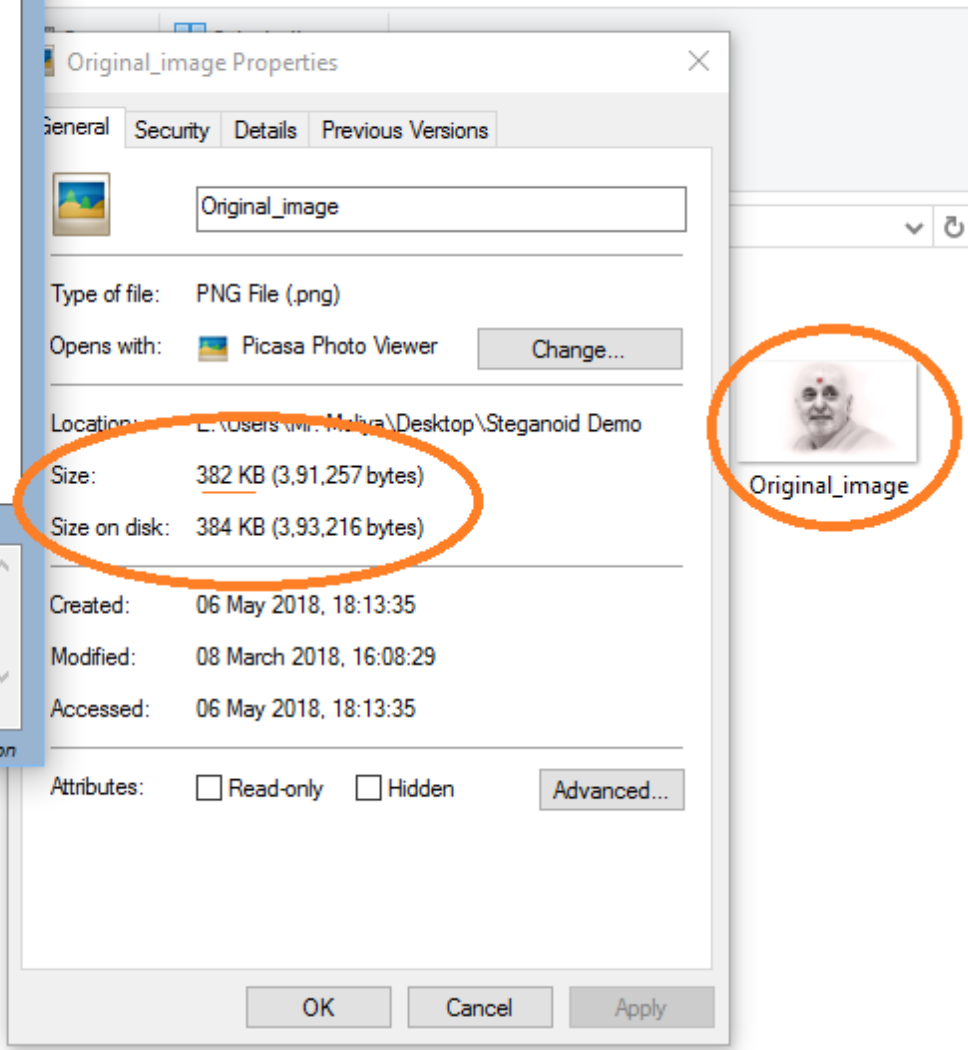
We require only 125crore x 600KB, (i.e. 750TB).

Benefits:

As per seen above example we can say we save 500 TB data. (500 TB = High cost)

User can hide data more than image size:





A tool for Steganography (1)

backup

It's **not a bug**. It's **a real Magic.**
In **382KB image** you can hide **1.02MB data.**

Why? :
Total number of pixel in this 382KB PNG file is = 1073800**(Very huge).**

Implementation

Successfully implemented…

- Language : C#
- Platform : Tested with all windows version(7, 8, 8.1, 10).
- Tools : Microsoft Visual Studio 2015, Microsoft Paint.

DEMO

Youtube Link:
https://www.youtube.com/watch?v=P9obmA9ws2I

Software link (Download and try):
https://github.com/HimanshuMoliya/Steganoid/blob/master/Steganoid%20-%201.0.exe

Future Scope and real life Application

In, future we add video steganography feature.

- Use as secret message transmission from one country to another country.
  E.g. Indian embassy Pakistan to India.

- Use in Military, CBI, RAW communication.
- Use in business communication and real life communication.
- As data minimization tool, As digital watermarking tool.

Thank You!

Himanshu Moliya
himanshu.moliya@iet.ahduni.edu.in

School of Engineering and Applied Science
Ahmedabad University