APPLICATION OF HIDING CRYPTED TEXT MESSAGES INTO IMAGE

(STEGANOGRAPHY)

Oğulcan Topsakal Jan 11, 2021
ogulcan.topsakal@gazi.edu.tr

BEFORE STEGANOGRAPHY: CRYPTOGRAPHY

- Cryptography is the study of secure communications techniques…
- It is closely associated to encryption…
- In addition, cryptography also covers the obfuscation of information in images…

Jan 11, 2021

On the other hand: steganography

- Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.

Jan 11, 2021

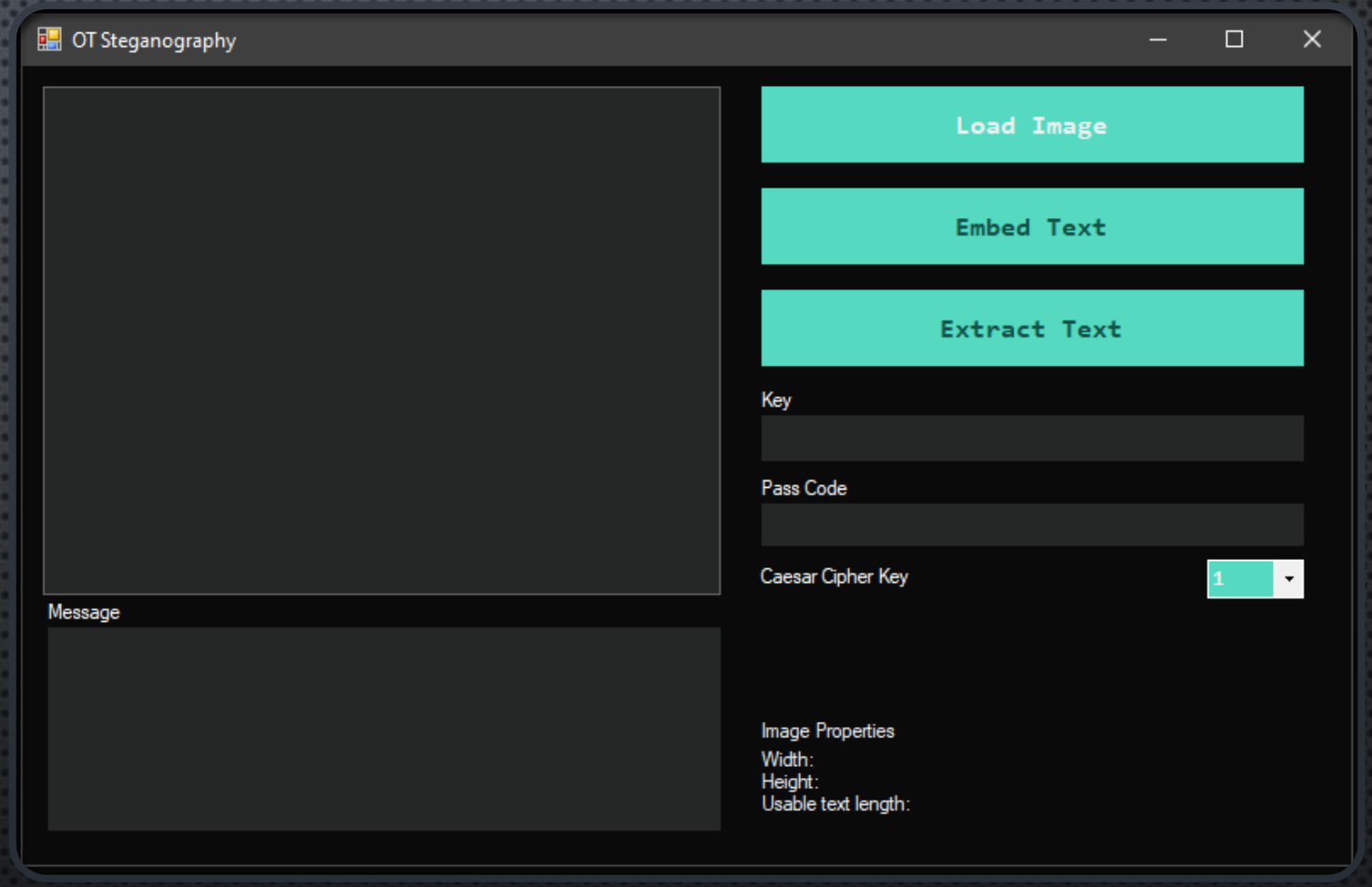
STEGANOGRAPHY IS DISTINCT FROM CRYPTOGRAPHY BUT..

- USING BOTH TOGETHER CAN HELP IMPROVE THE SECURITY OF THE PROTECTED INFORMATION AND PREVENT DETECTION OF THE SECRET COMMUNICATION

Jan 11, 2021

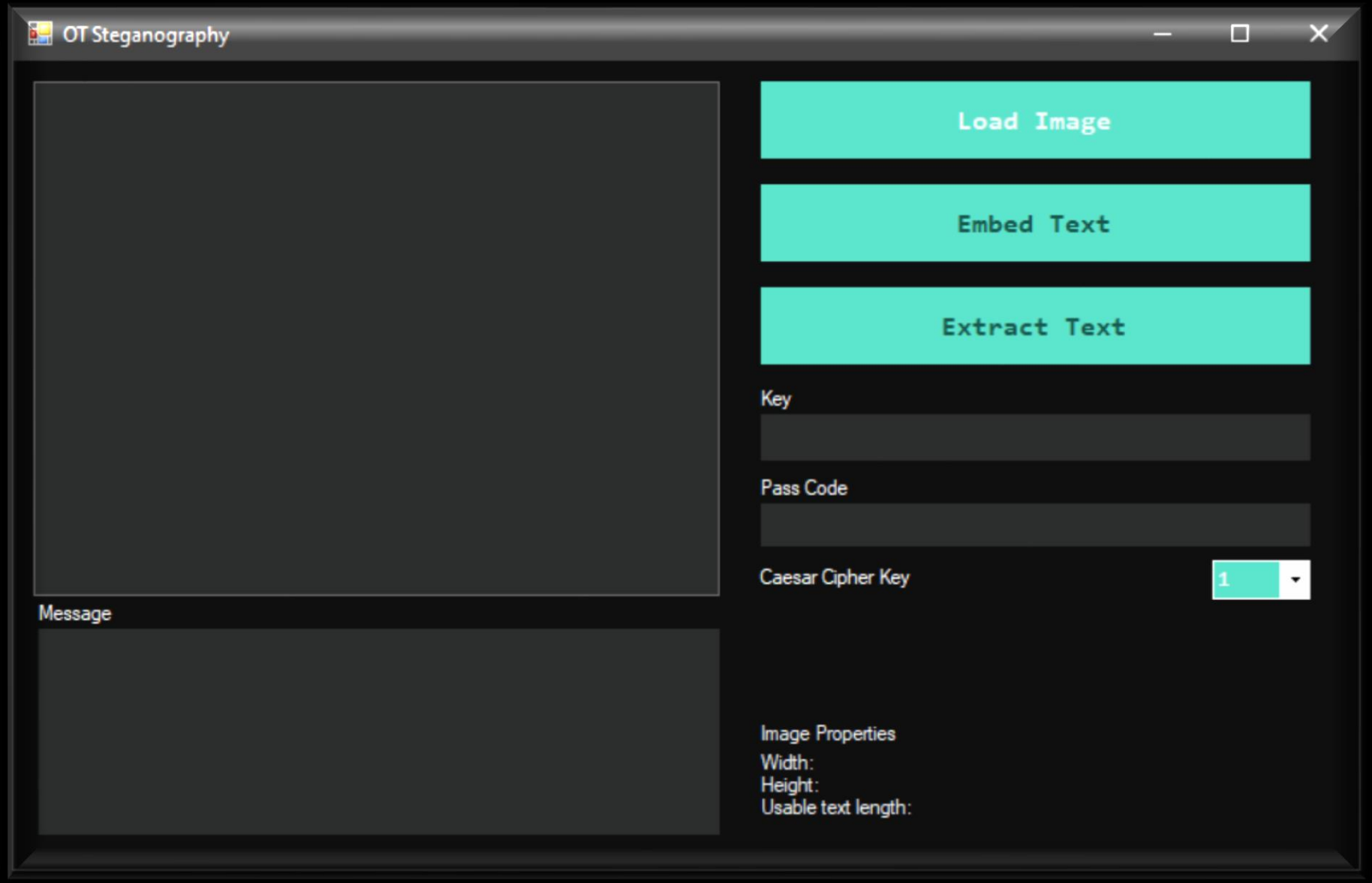
MODEL AND IMPLEMENTATION

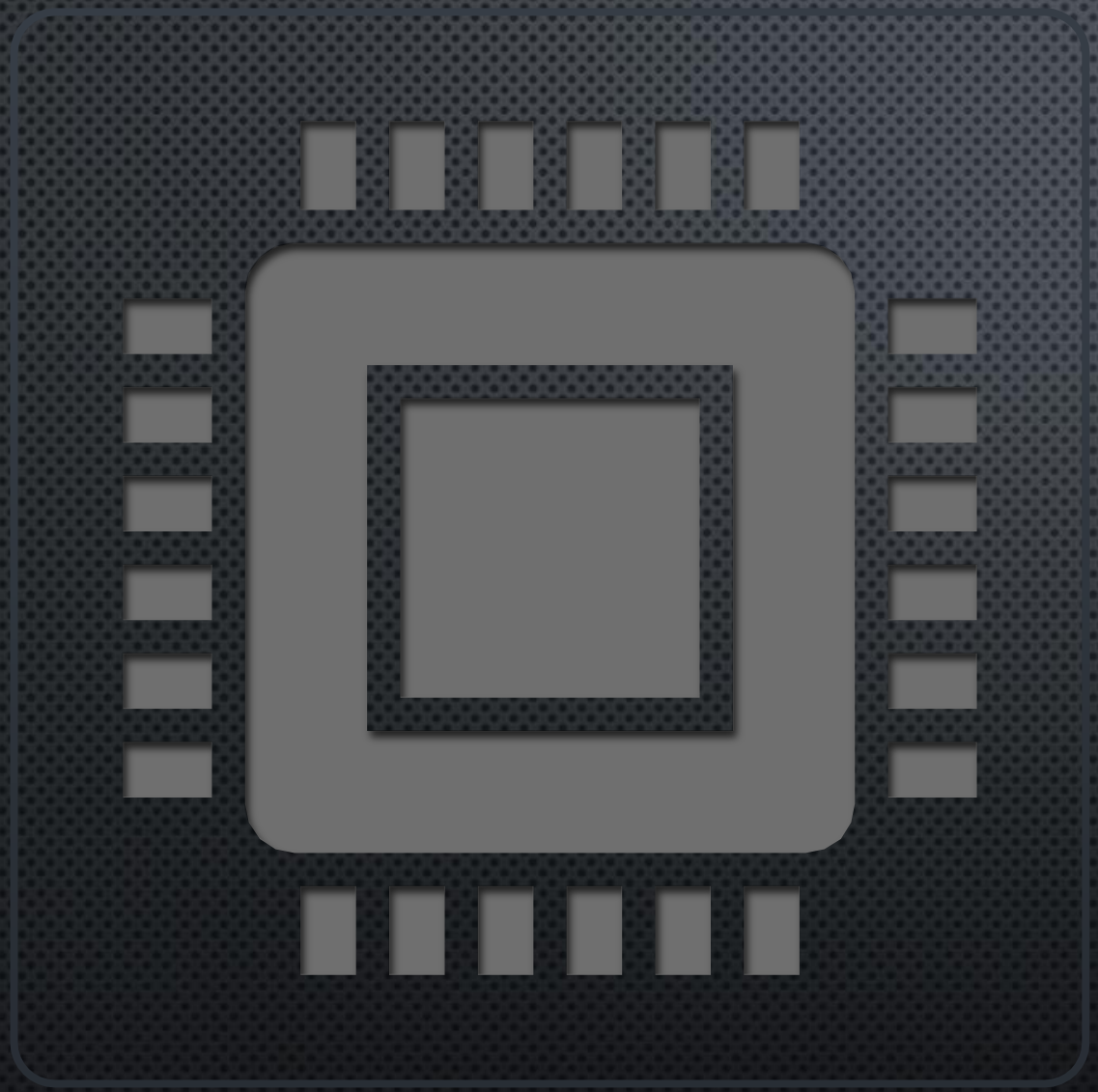
- USER INTERFACE
- METHODS&ALGORITHMS



Jan 11, 2021

User Interface





ON BACKEND

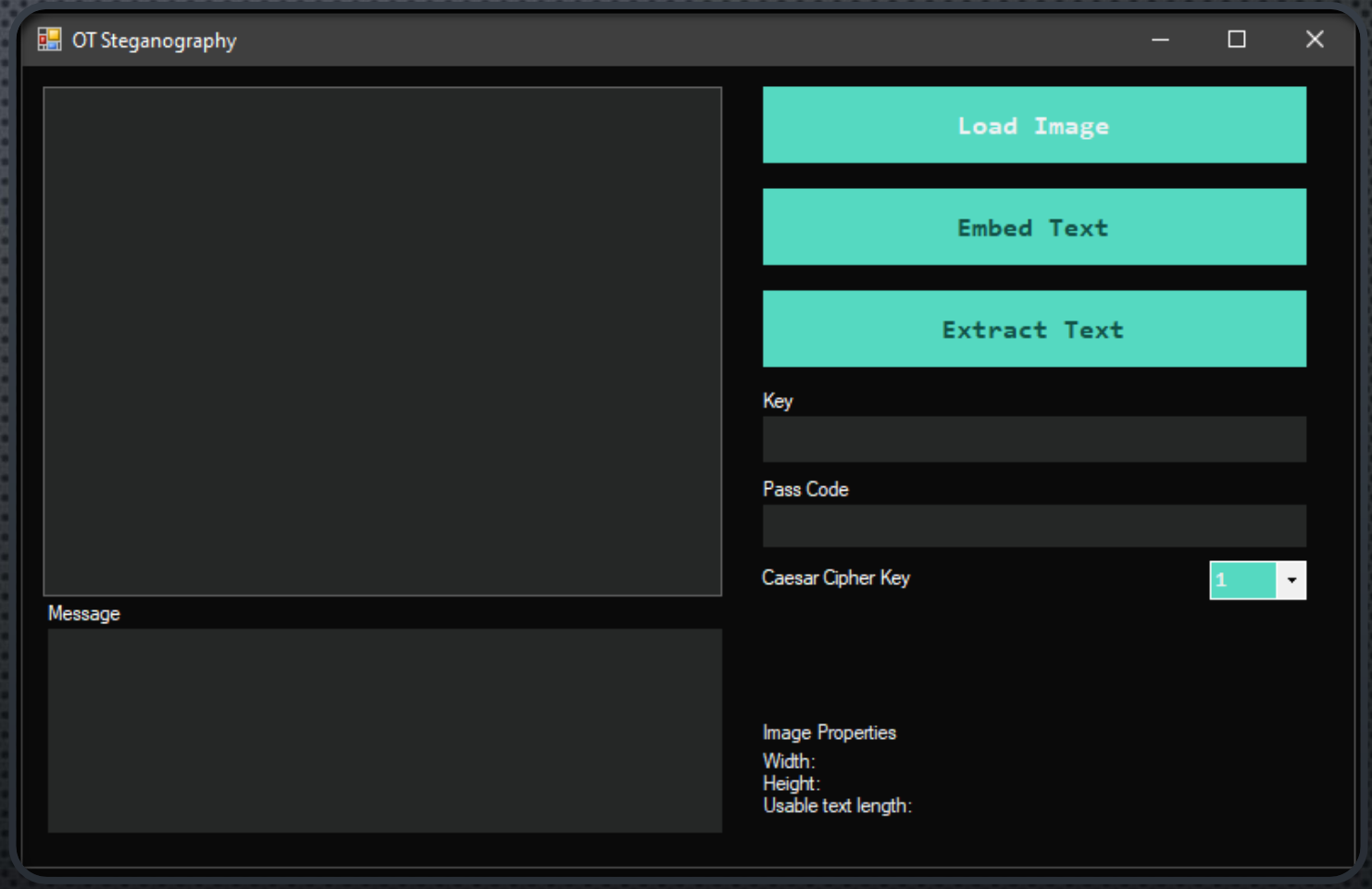
- There are 3 main algorithm running on background
  - Steganography Algorithm
  - Caesar Cipher Algorithm
  - Key Cryptography Algorithm

Jan 11, 2021

STEGANOGRAPHY ALGORITHM

Embedding Algorithm pseudocode:

1. Take text(message) input from user.
2. Take image from user and convert this image to a bitmap and calculate boundaries of this bitmap to understand limitations of maximum message can be hidden.
3. Cipher text input using Caesar Cipher Algorithm with selected key from user.
4. Convert text input string to binary string (“Example”) -> (“101010”).
5. Generate random start point with using the bounds which calculated at second step.
6. Visit pixels and put pixel’s lsb to our crypted binary data one by one until reach the length of binary string.
7. Create new image with embedded message bitmap. Use png extension to prevent data loss.
8. Generate text file which includes key, pass code and Caesar cipher key.
9. End.

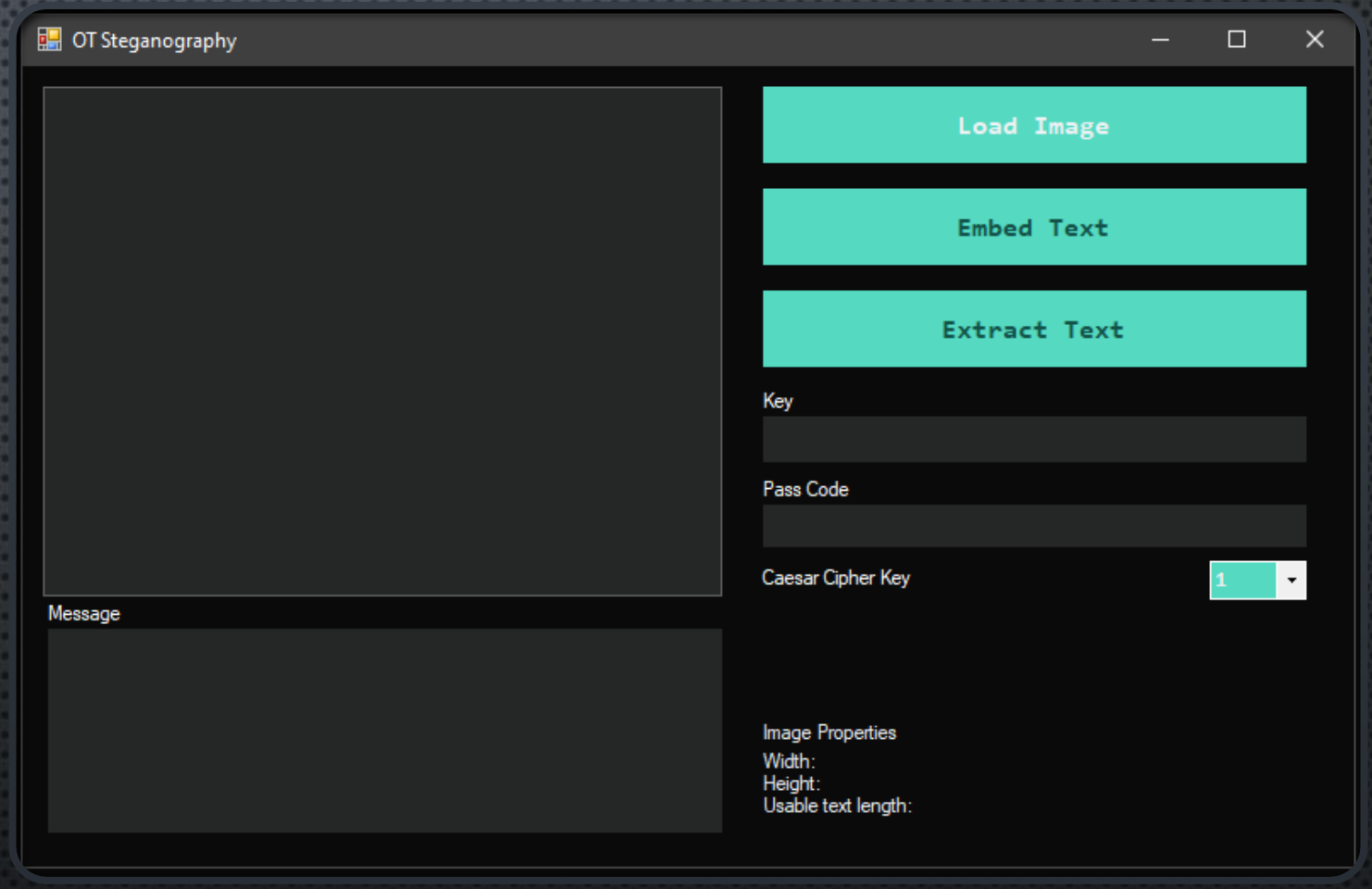


Jan 11, 2021

STEGANOGRAPHY ALGORITHM

Extracting Algorithm pseudocode:

1.Take text decryption key from user.
2.Take pass code from user.
3.Take Caesar cipher key from user to use it last step.
4.Take image which includes hidden message from user.
5.Check if these values is true. If not show dumb message.
6.If values are correct start decryption.
7.Extract starting and end point from decrypted key.
8.Convert given image to bitmap.
9.Go to start point pixel of bitmap with using decrypted points.
10.Read least significant bits of pixels until reaching end point.
11.Store all bits inside string.
12.Convert the binary string by reading 8 bits by 8 bits.
13.Decipher string with using Caesar cipher key from we take at step 3.
14.Show last product to user.



Jan 11, 2021

CAESAR ALGORITHM

1

Caesar Algorithm Encipher pseudocode:

1.Take command line arguments for string to be encoded and an integer as a cipher key.
2.Loop through each character in input string, change value by the value of the cipher.
3.Return out encrypted string.

2

Caesar Algorithm Decipher pseudocode:

1.Take command line arguments for string to be decoded and an integer as a cipher key.
2.Loop through each character in input string, change value by the value of the cipher.
3.Return out decrypted string.

Jan 11, 2021

KEY CRYPTOGRAPHY ALGORITHM

1

Text Cryptography Algorithm Encrypt pseudocode:

1.Generate random 256bit, store this value in salt.
2.Generate random 256bit, store this value in iv.
3.Encode user input with UTF8.
4.Generate password with using Rfc2898DeriveBytes.
5.Return crypted string.

2

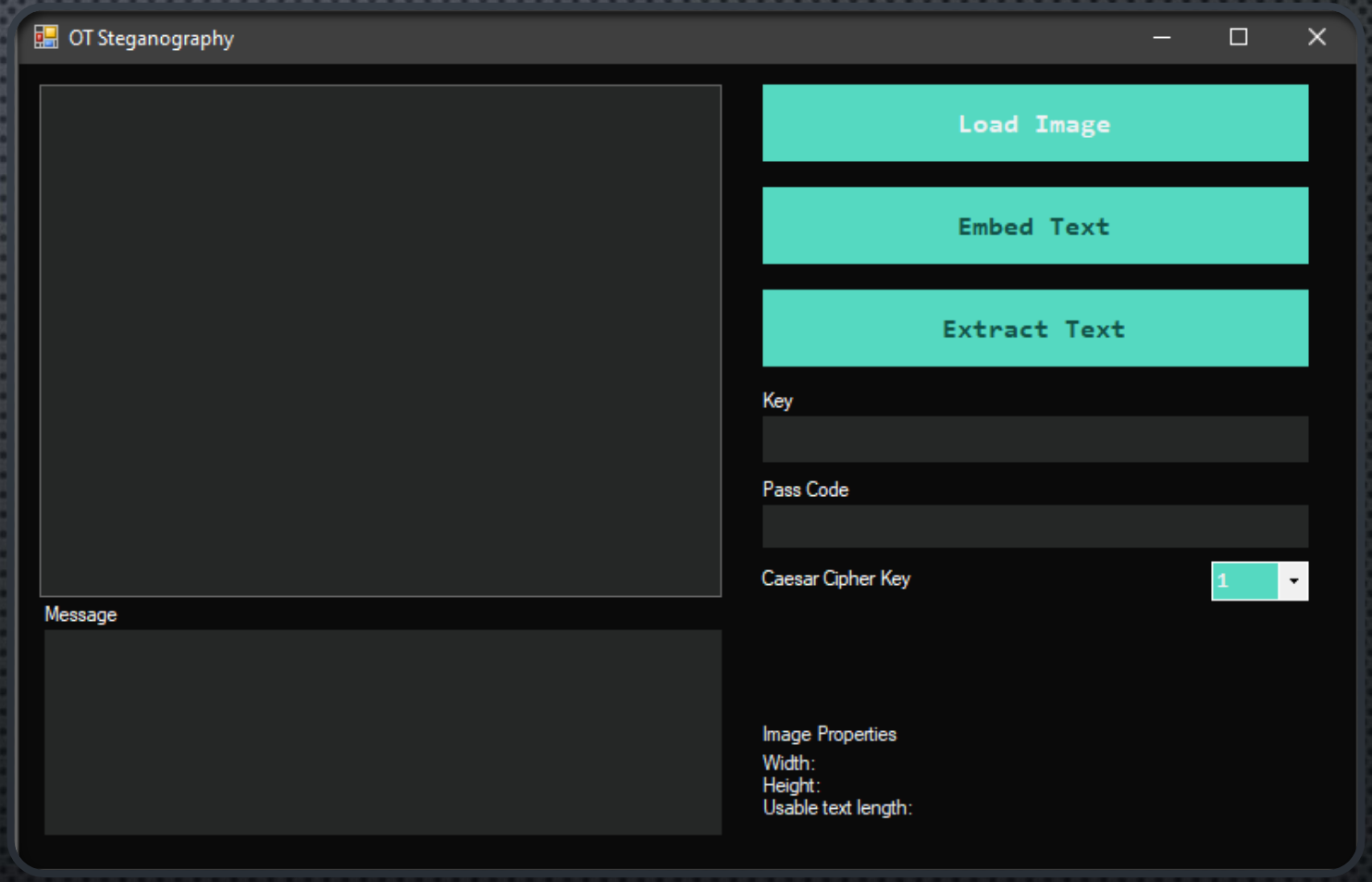
Text Cryptography Algorithm Decrypt pseudocode:

1.Convert cipher text from base 64 string.
2.Split converted cipher text as salt, iv and cipher text bytes.
3.Generate string with using Rfc2898DeriveBytes.
4.Return decrypted string.

Jan 11, 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

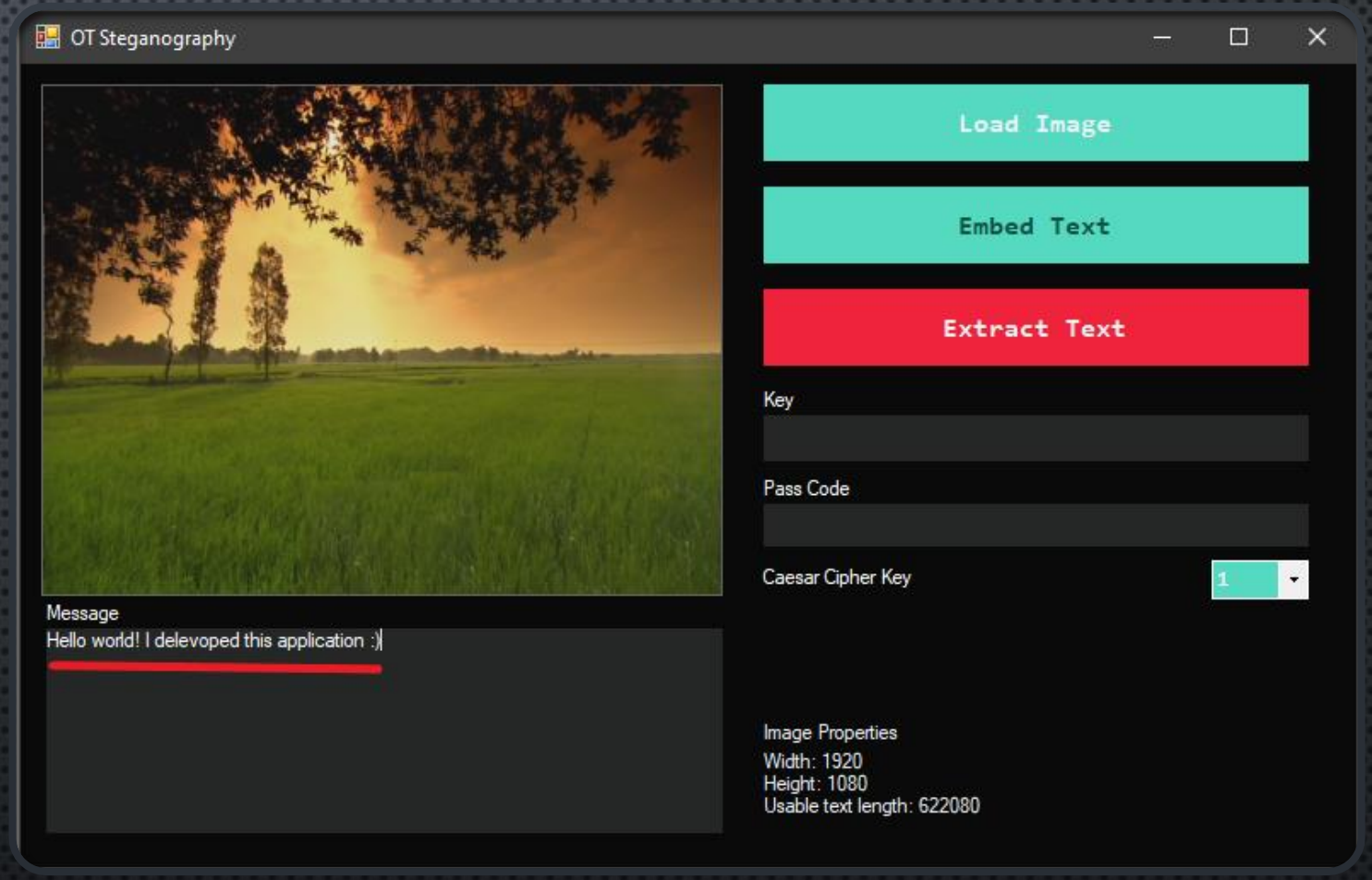
1. First click load image button to select sketch picture.



Jan 11, 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

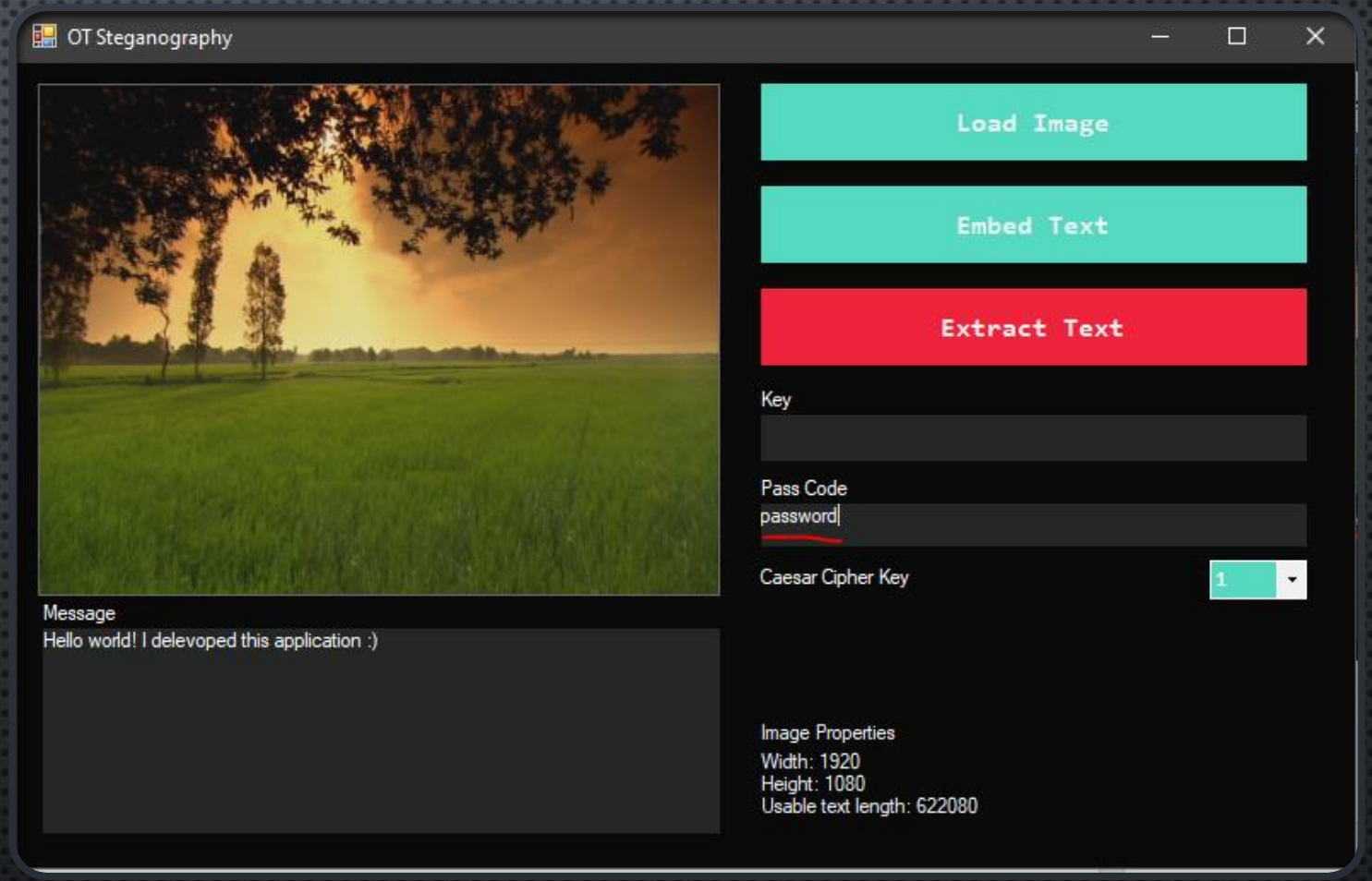
2. WRITE THE MESSAGE YOU WANT TO BE HIDDEN IN THE MESSAGE FIELD.



Jan 11, 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

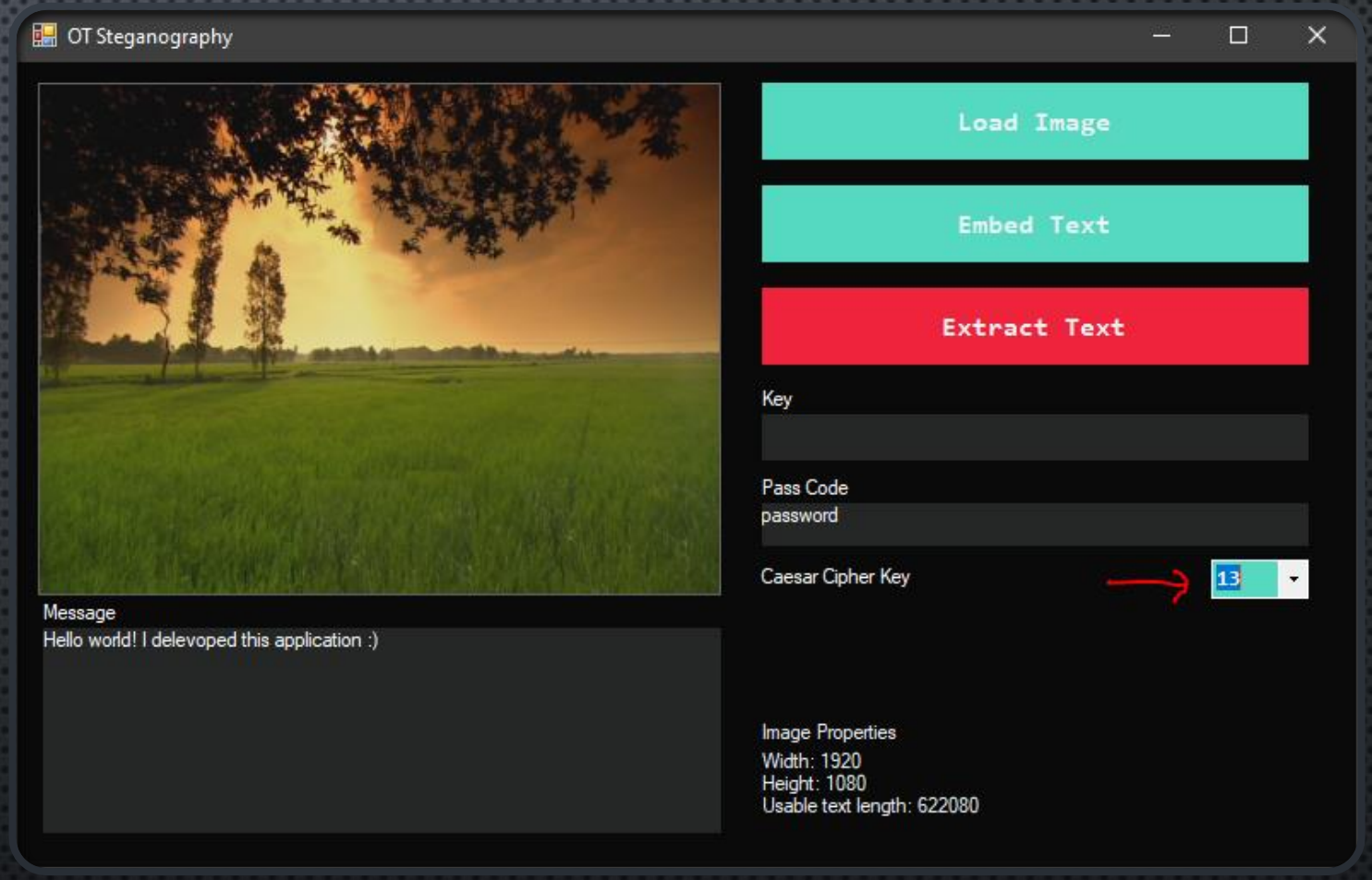
3. ENTER A STRONG PASSWORD –AS I DO- TO PERSONALIZE YOUR OPERATION.



Jan 11, 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

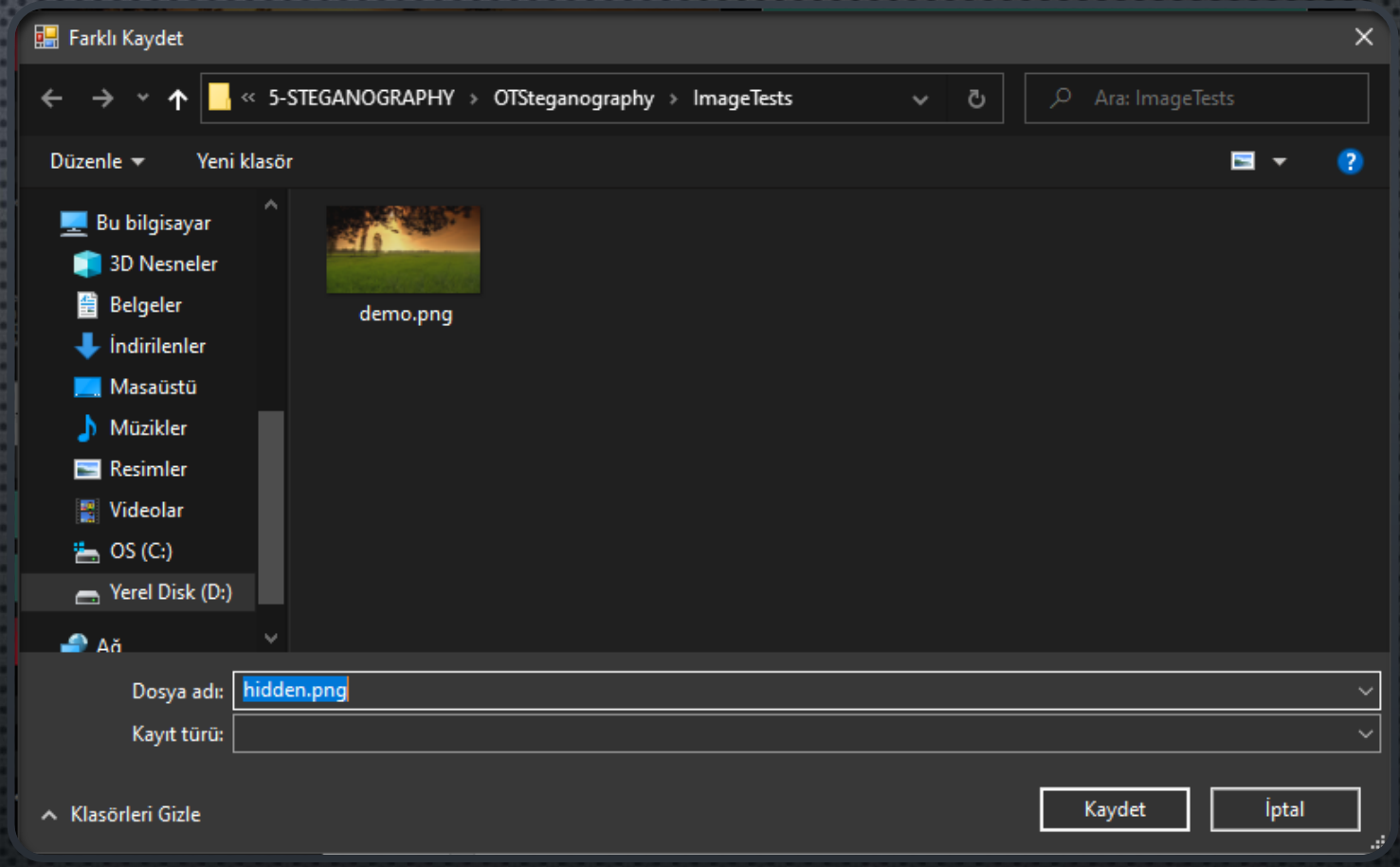
4. SELECT CAESAR CIPHER KEY TO CIPHER YOUR TEXT MESSAGE BEFORE EMBEDDING INTO PICTURE.



11 Ocak 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

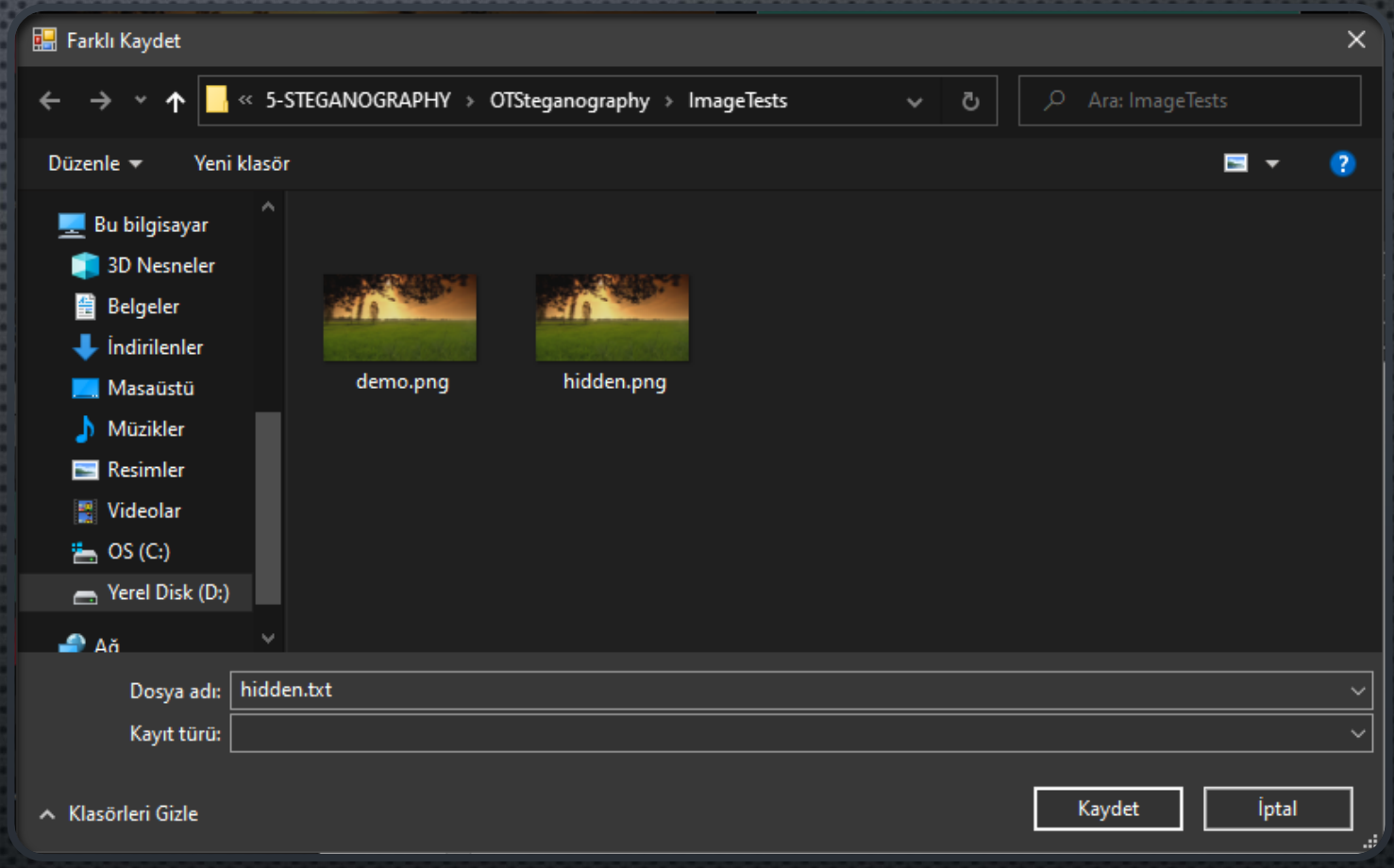
5. CLICK EMBED TEXT BUTTON AND GIVE A NAME TO NEW IMAGE WILL BE CREATED.



Jan 11, 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

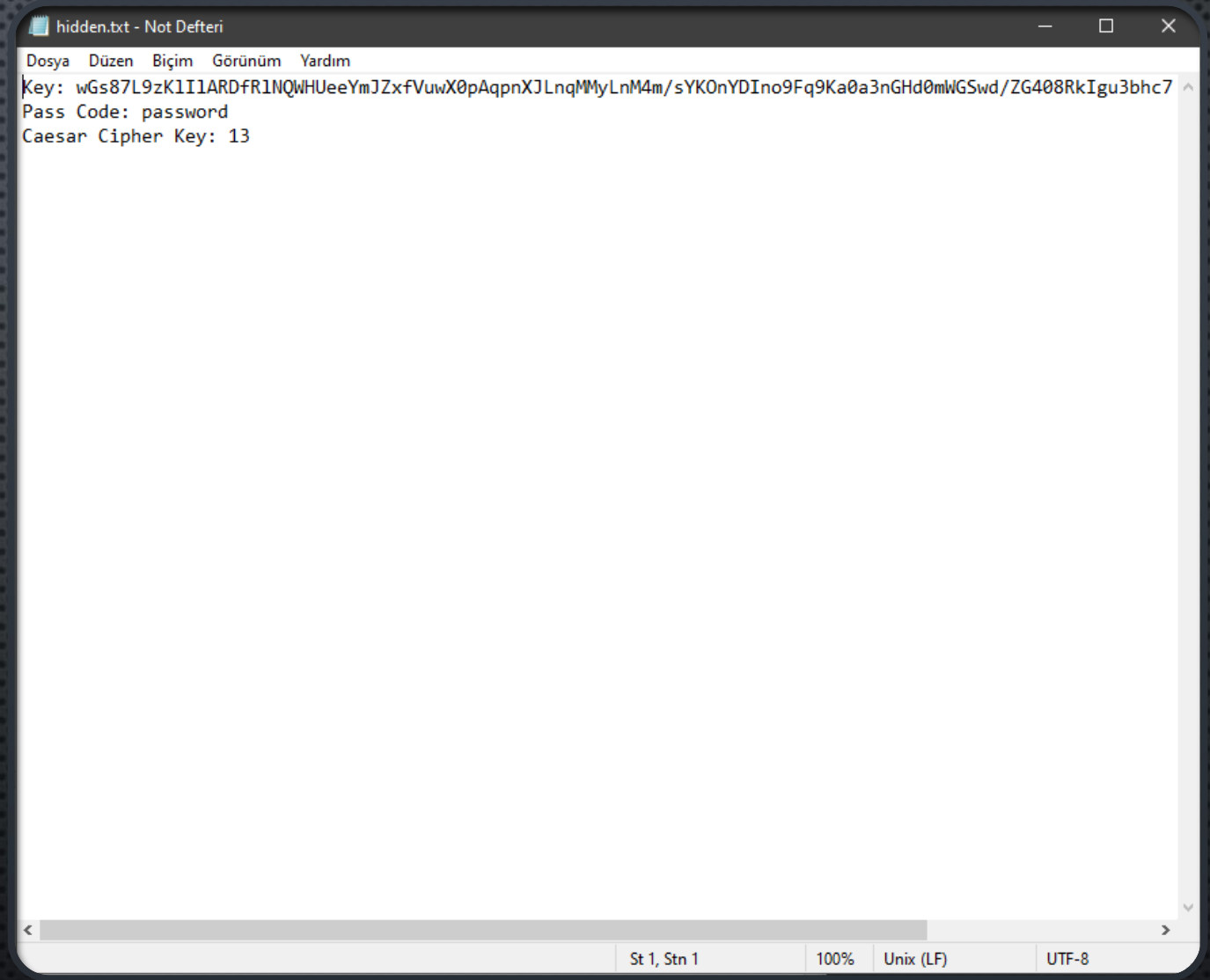
6. GIVE A NAME TO A TEXT PRODUCT. TEXT PRODUCT INCLUDES THESE; KEY, PASS CODE AND CAESAR CIPHER KEY.



Jan 11, 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

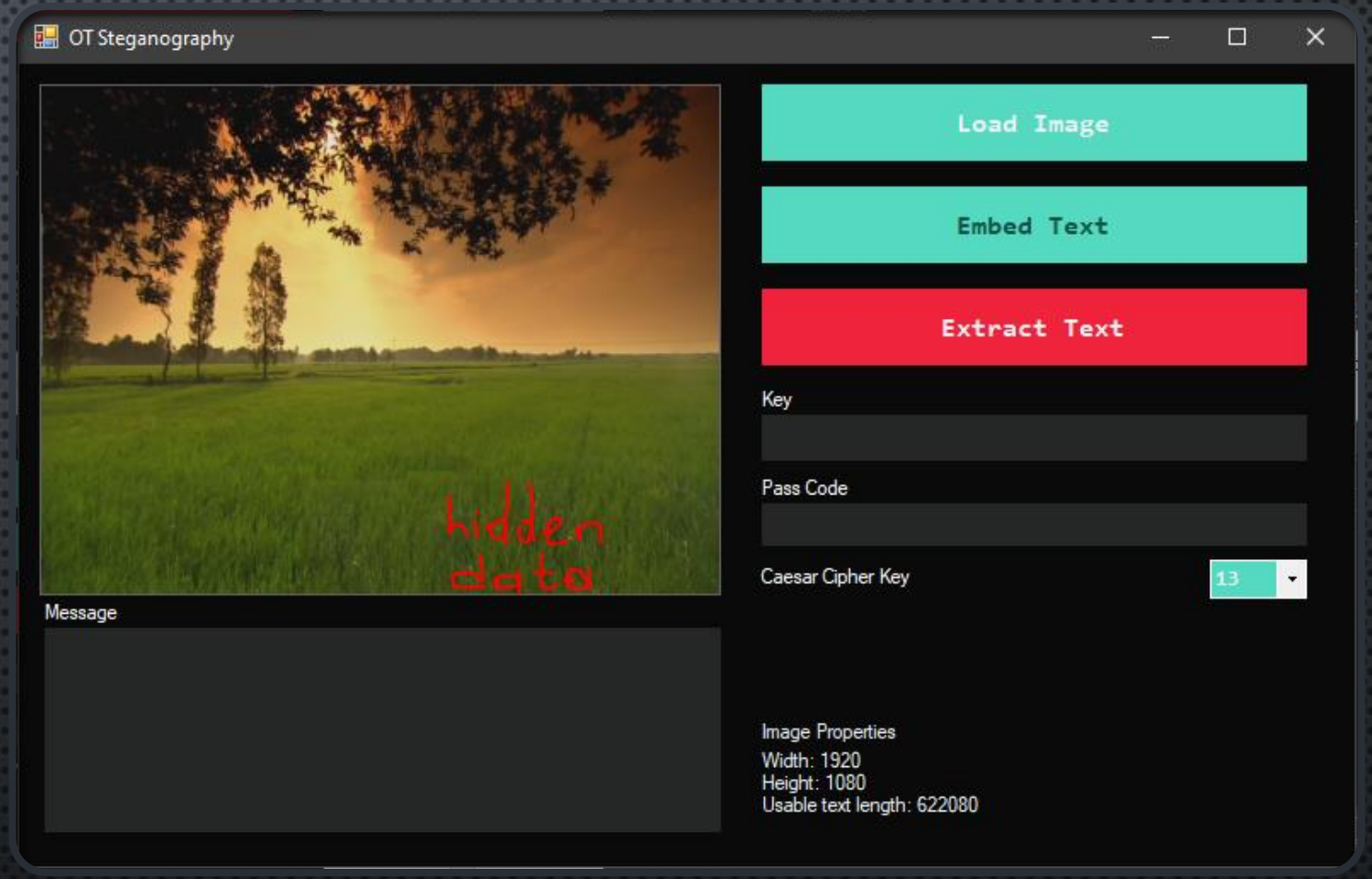
7. THIS IS TEXT PRODUCT CREATED BY PROGRAM.



Jan 11, 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

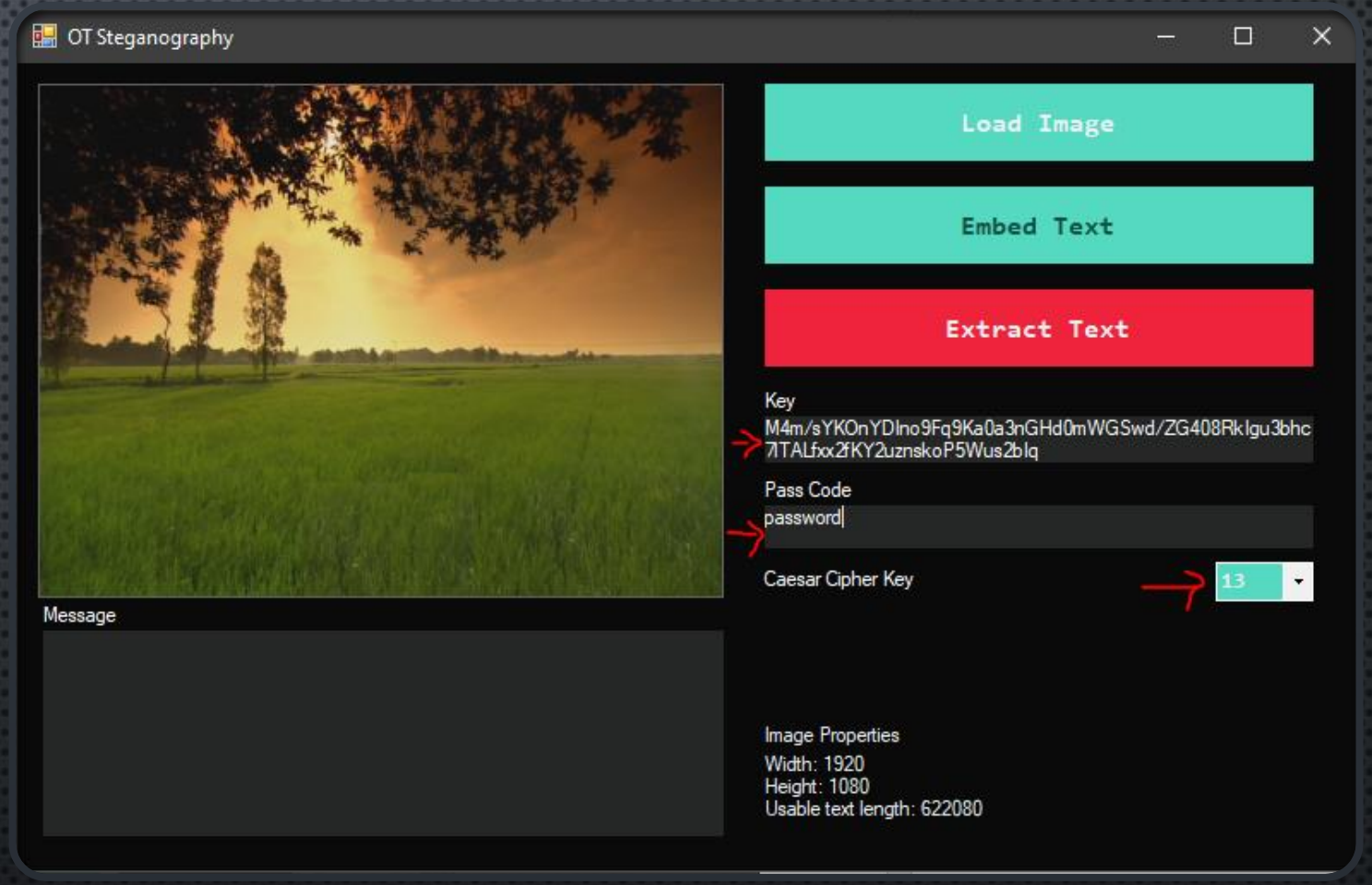
8. CLICK LOAD IMAGE BUTTON TO LOAD IMAGE WHICH HAS CRYPTED DATA.



Jan 11, 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

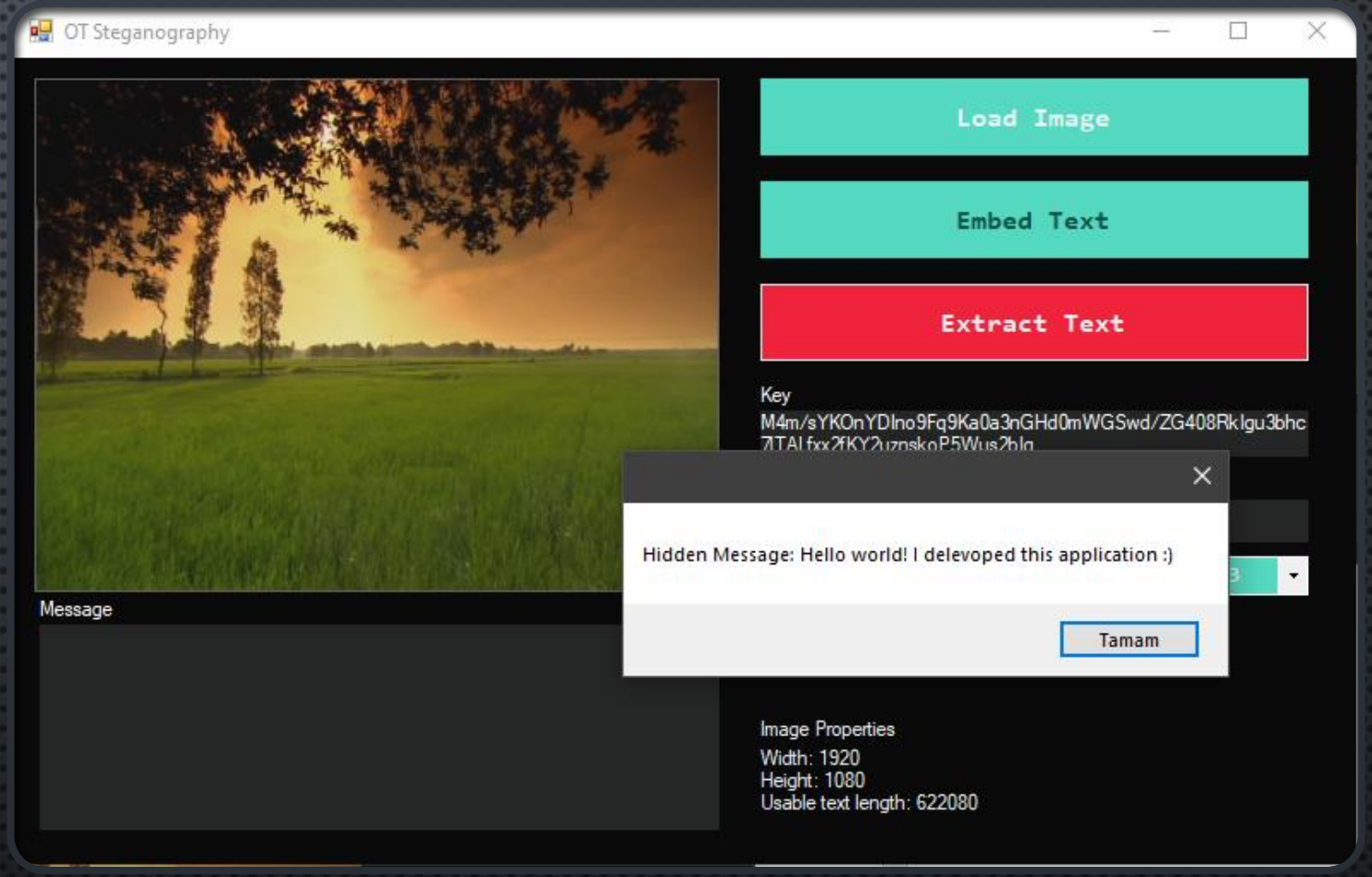
9. ENTER YOUR KEY, PASS CODE AND CAESAR CIPHER KEY CORRECTLY ON UI BEFORE CLICKING EXTRACT TEXT.



Jan 11, 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

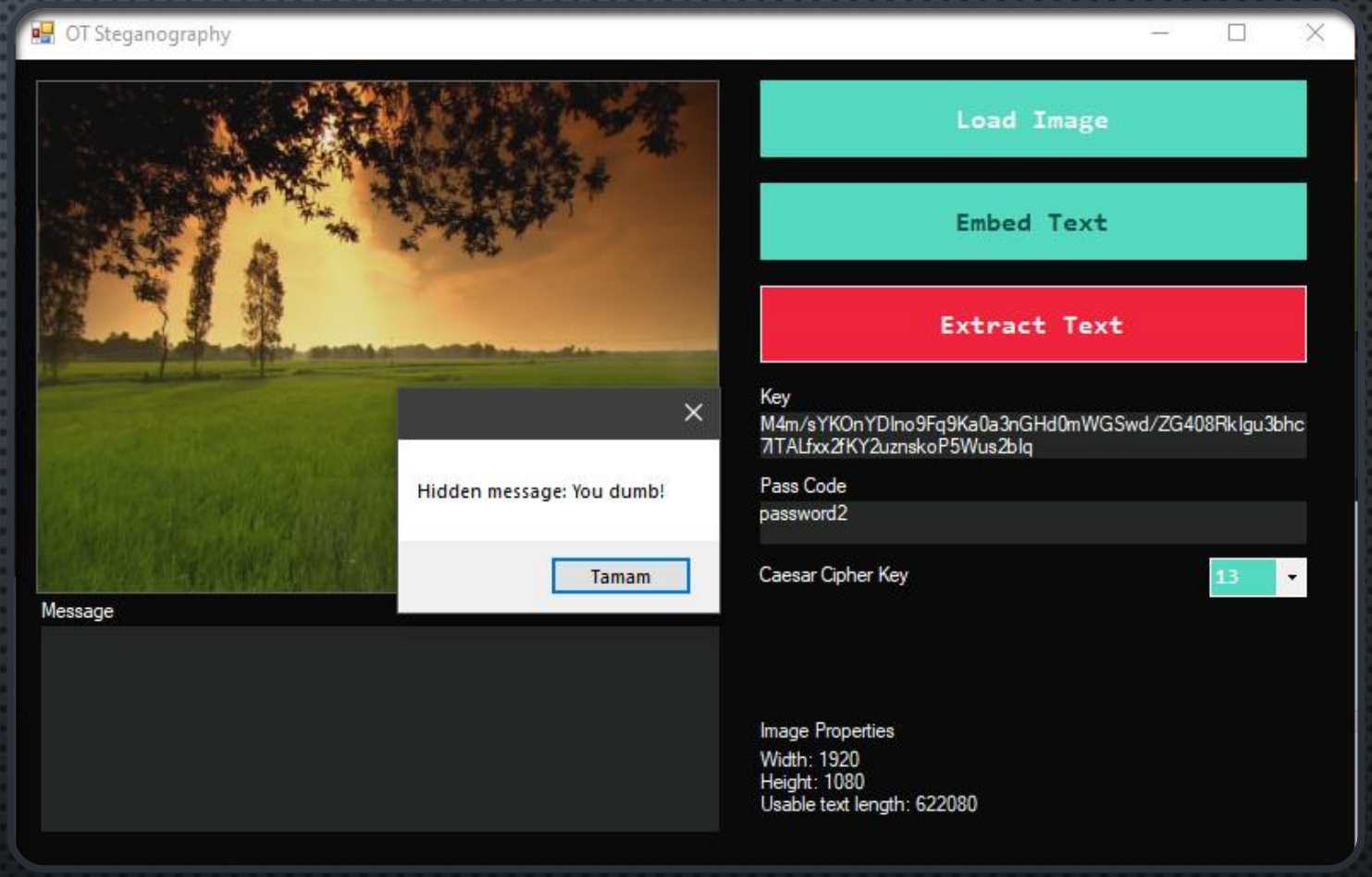
10. CLICK EXTRACT TEXT BUTTON.



Jan 11, 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

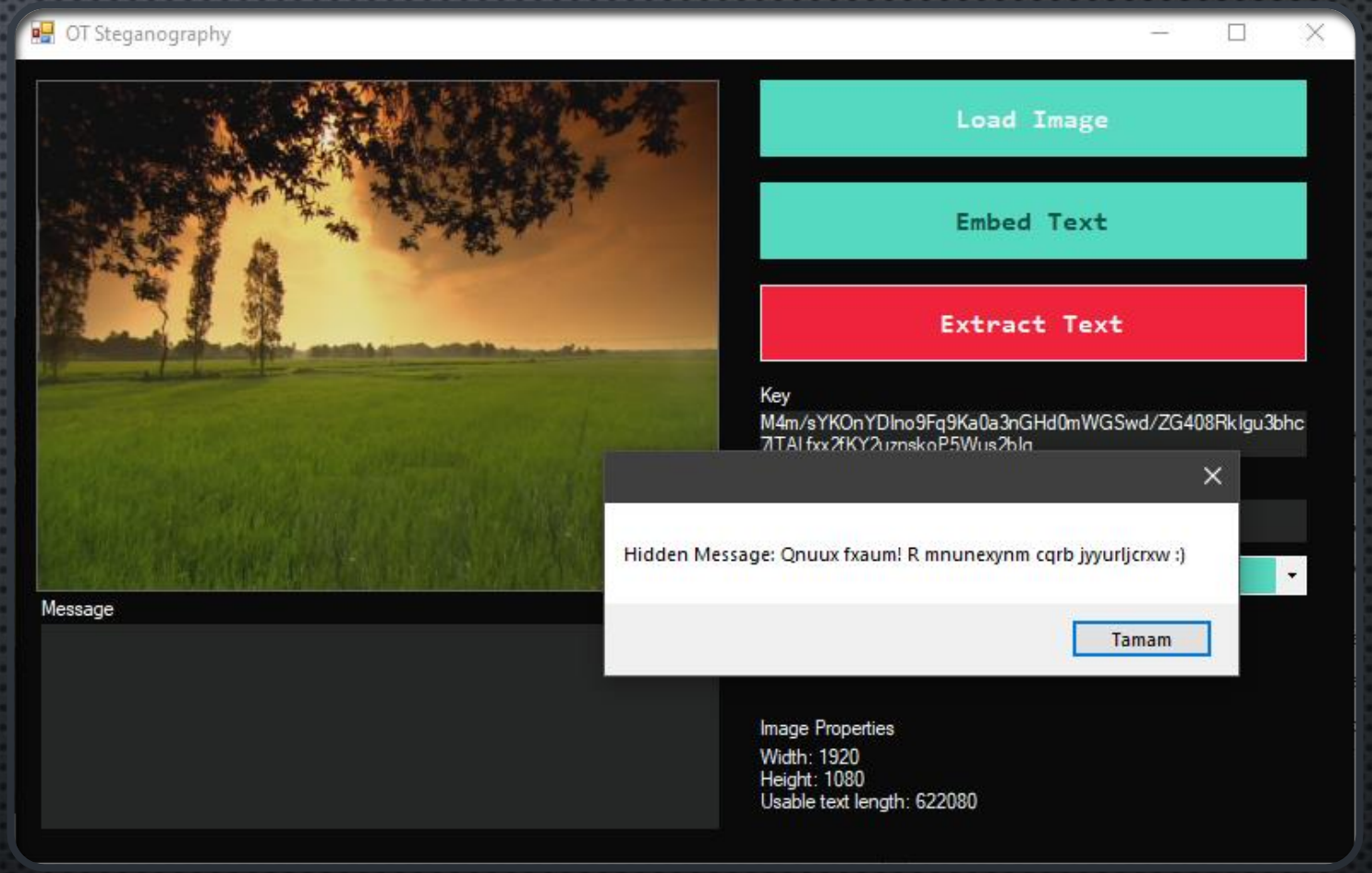
11. WHAT IF ANY OF THESE FIELD ENTERED WRONG.



Jan 11, 2021

STEP BY STEP HIDING MOST SECRET MESSAGE

11. WHAT IF ANY OF THESE FIELD ENTERED WRONG.



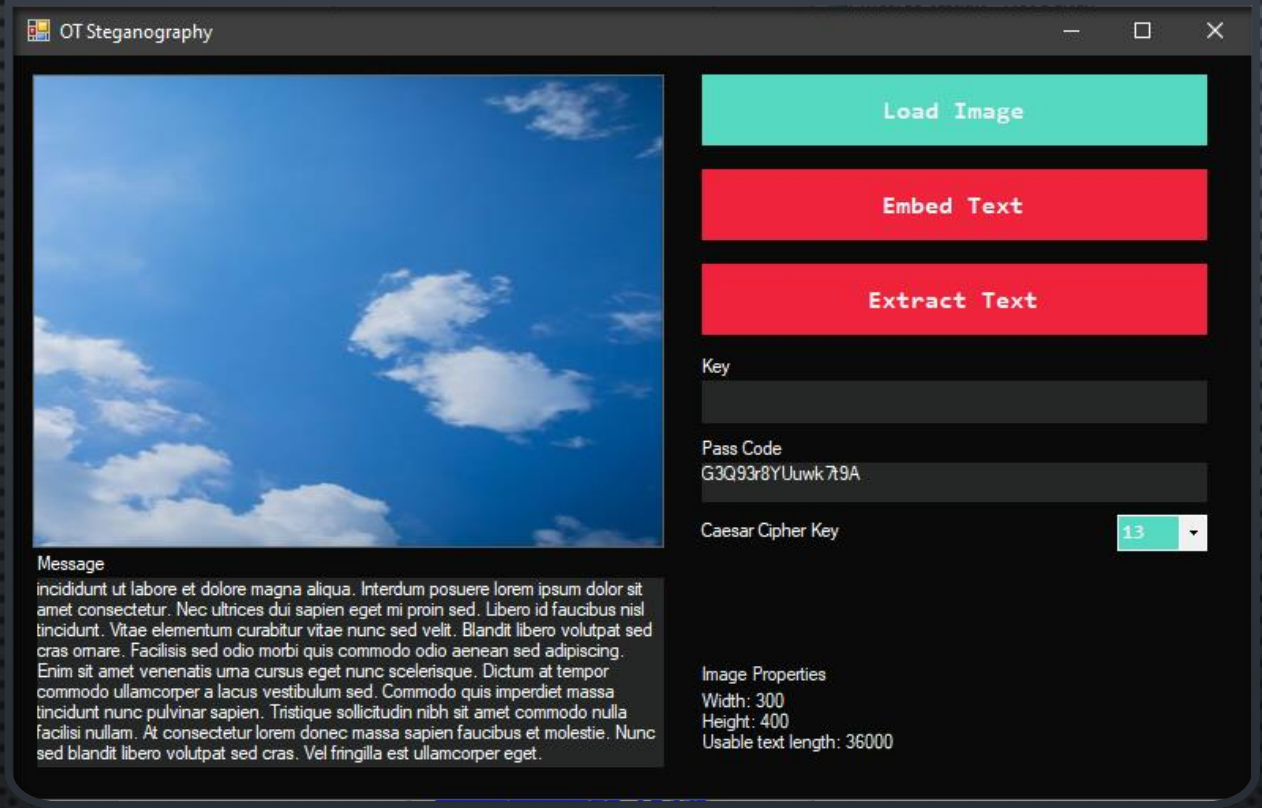
Jan 11, 2021

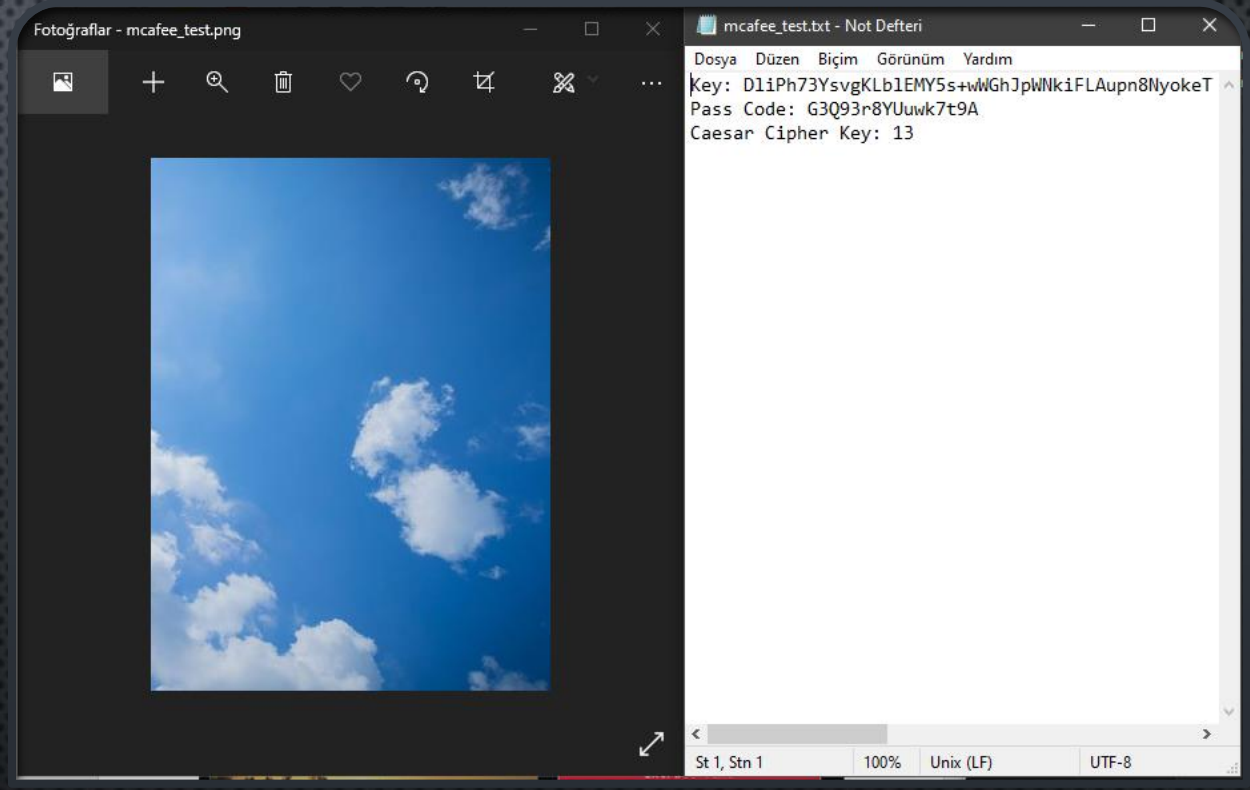
ANALYSIS

- There are several ways to test how undetectable this program. The first of these is "STEGANOGRAPHY DEFENSE INITIATIVE", mcafee antivirus program offers online.

Jan 11, 2021

PS. I USED SAME DATA ON ALL ANALYSIS STEPS





Jan 11, 2021

RESULTS

Suspicious: No - We can't find significant traces of steganography in this image
Confidence Level: Medium
Score: 12.897532401822827
Scan Time: 2566 ms
Errors: false

MCAFEE RESULT

Jan 11, 2021

NOISE ANALYSIS

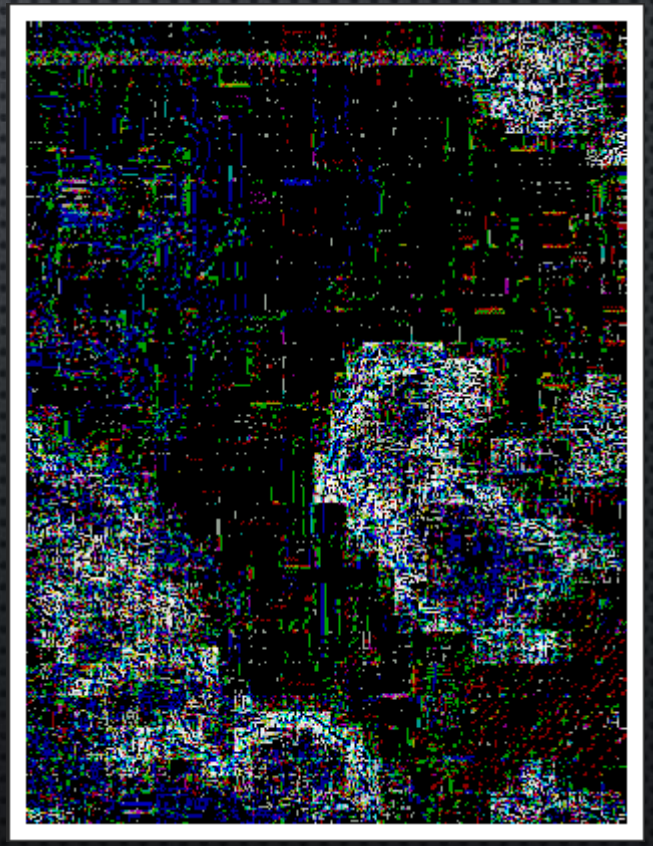
- NEXT ANALYSIS IS EXAMINING NOISE ON ORIGINAL IMAGE AND LAST PRODUCT. CURRENT STATE OF THIS APPLICATION DOES NOT SUPPORT ADDING RANDOM NOISE ON PRODUCT IMAGE.

Jan 11, 2021

AS YOU CAN SEE ON FINAL PRODUCT NOISE ANALYSIS IMAGE, WHERE THE DATA IS HIDDEN IS CLEARLY VISIBLE.

Original Image

Jan 11, 2021



Final Product

Own analysis tool (python)

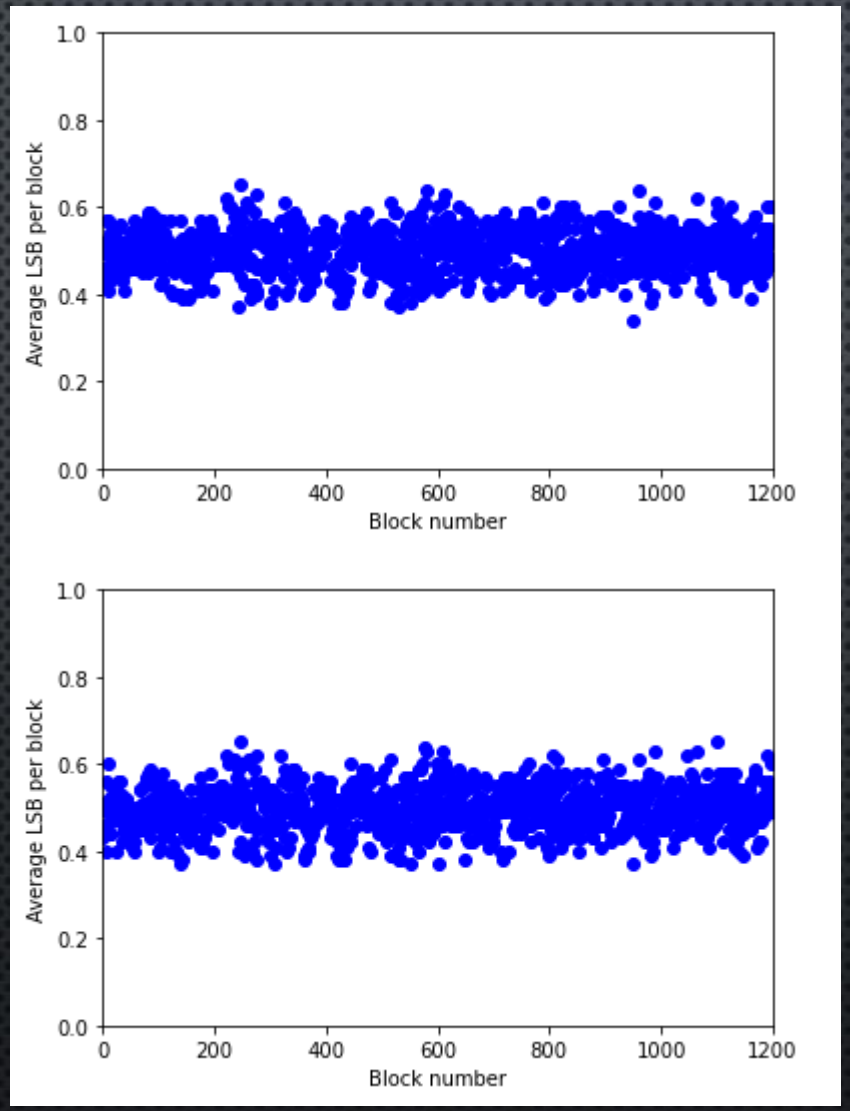
- I developed small analysis tool to maybe I detect hidden data as well. But on the first step I need original image to compare/find hidden data. This analysis does not work at real world for sure.
- First, I calculated mean squared error and structural similarity on these images.

Jan 11, 2021

We can see 0.02 which is very small mean squared error. After this I checked average least significant bits per blocks. Block size is 100 pixel.

Jan 11, 2021

After this process still no significant difference can seen. It may caused by message size. I used small one paragraph data to hide.



Jan 11, 2021

Outro

- Information hiding techniques received very much less attention from the research community and from industry than cryptography.
- Steganography has its place in security. It is not intended to replace cryptography but supplement it.
- It can be clearly observed in this project that these two terms, when used together, reinforce each other.

Outro

- Steganography software is used to perform a variety of functions in order to hide data, including encoding the data in order to prepare it to be hidden inside another file, keeping track of which bits of the cover text file contain hidden data, encrypting the data to be hidden and extracting hidden data by its intended recipient.
- Steganography is still a reliable way to hide your data today. Especially using different encryption algorithms with steganography would be a logical choice for more difficult decryption of data.

THANKS