International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 05 Issue 01 | 2020

Enhancing Data Security Using Steganography with Python

Karan Anand
MCA Scholar, School of CS & IT, Dept. of MCA Jain (Deemed-to-be University)-560069

ABSTRACT

Steganography is the specialty of concealing how correspondence is going on, by covering data in other data. A wide extent of transporter record affiliations can be utilized, yet modernized pictures are the most standard thinking about their rehash on the web. For concealing mystery data in pictures, there exists a massive assortment of steganography procedures some are greater than others and every one of them has particular solid and feeble centre interests. Various applications may need overall hereticalness of the mystery data, while others require a huge question message to be disguised. This undertaking report expects to give a review of picture steganography, its uses, and methods. It also attempts to perceive the necessities of a decent steganography check and quickly examines which steganographic methodologies are intelligently reasonable for which applications.

Keyword: -Steganography, Python, data security, Decoding-Algorithm

1. INTRODUCTION

The subject that is chosen is Steganography Using Python, one explanation that gatecrashers can be productive is most of the information they get from a system is in a structure that they can examine and comprehend. Interlopers may reveal the information to others, change it to twist an individual or affiliation, or use it to dispatch an attack. One response for this issue is, utilizing steganography. Steganography is a strategy for hiding information in modernized media. Instead of cryptography, it isn't to shield others from knowing the disguised information yet it is to shield others from envisioning that the information even exists. Steganography become logically critical as more people join the web change. Steganography is the art of concealing information in habits that prevents the distinguishing proof of covered messages. Steganography fuse an assortment of riddle specific systems that disguise the message from being seen or found. Due to impel in ICT, by far most of information is kept electronically. Subsequently, the security of information has become a chief issue. Other than cryptography, steganography can be used to ensure about information. In cryptography, the message or encoded message is embedded in a serious host before going it through the framework, as such the presence of the message is dark. Other than covering data for protection, this strategy of information stowing ceaselessly can be contacted copyright protection for cutting edge media: sound, video and pictures.

This endeavour gives nuances how to share data using steganography. The creating possibilities of current trades need the remarkable strategies for security especially on PC mastermind. The framework security is getting continuously noteworthy as the amount of data being exchanged on the web increases. Thusly, the order and data decency are needing to guarantee against unapproved access and use. This has achieved a sensitive improvement of the field of information concealing Information concealing is a rising investigation region, which incorporates applications, for instance, copyright protection for cutting edge media, watermarking, fingerprinting, and steganography.

In watermarking applications, the message contains information, for instance, owner distinctive evidence and a modernized time stamp, which typically applied for copyright affirmation. Unique mark, the owner of the educational file embeds a successive number that astoundingly perceives the customer of the instructive record. This adds to copyright information to makes it possible to follow any unapproved used of the educational assortment back to the customer. Steganography conceal the release message inside the host enlightening assortment and closeness immaterial and is to be constantly granted to a gatherer. The host instructive file is intentionally contaminated, anyway in an in-disguise way, planned to be impalpable to an information assessment.

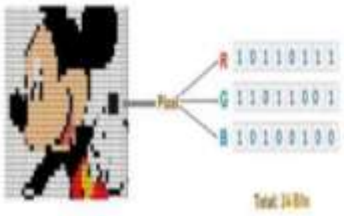
2. HISTORY

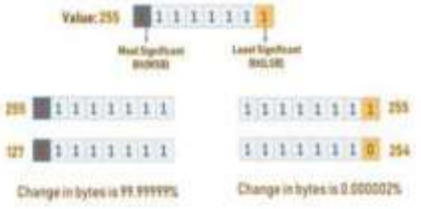
The primary recorded employments of steganography can be followed back to 440 BC in Greece, when Herodotus makes reference to two models in his Histories. Histiaeus made an impression on his vassal, Aristagoras, by shaving the top of his most confided in worker, "denoting" the message onto his scalp, at that point sending him out the door once his hair had regrown, with the guidance, "When thou craftsmanship come to Miletus, offer Aristagoras shave thy head, and look consequently." Additionally, Demaratus sent an admonition about an impending assault to Greece by composing it straightforwardly on the wooden support of a wax tablet prior to applying its beeswax surface. Wax tablets were in like manner utilize then as reusable composing surfaces, here and there utilized for shorthand.

In his work Polygraphies, Johannes Trithemius built up his supposed "Ave-Maria-Cipher" that can shroud data in a Latin recognition of God. "Auctor Sapientissimus Conseruans Angelica Deferat Nobis Charitas Potentissimi Creatoris" for instance contains the disguised word VICIPEDIA.

3. ADVANTAGES OF STEGANOGRAPHY

Up to now, cryptography has consistently had its definitive job in ensuring the mystery between the sender and the planned collector. Be that as it may, these days' steganography methods are utilized progressively other than cryptography to add increasingly defensive layers to the concealed information. The benefit of utilizing steganography over cryptography alone is that the planned mystery message doesn't stand out to itself as an object of examination. Evidently obvious encoded messages, regardless of how unbreakable they are, stimulate intrigue and may in themselves be implicating in nations in which encryption is unlawful.

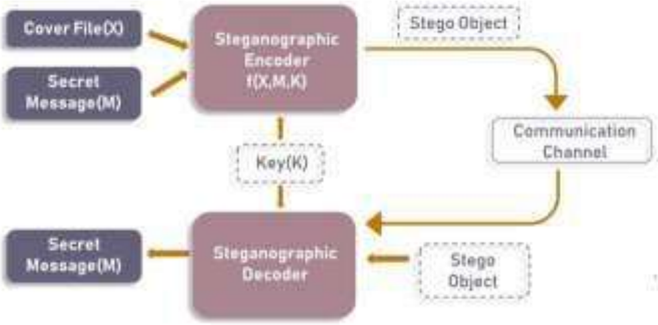



Value: 255
1 1 1 1 1 1 1
Most Significant Bit(MSB)
Least Significant Bit(LSB)
255
1 1 1 1 1 1 1
127
1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
255
1 1 1 1 1 1 1 0
254
Change in bytes is 99.99999%
Change in bytes is 0.000002%

4. TYPES OF STEGAN

Exactly when a customer types a URL in the web program then the program sends a requesting to the web worker. By and by when web worker gets a sale from the program, it first looks for the treats. In case treat isn't there, by then it makes a treat with a novel id for the given sales and subsequently passes it to the customer. The treat is taken care of on the customer's hard plate. By then various settings similarly as tendencies are furthermore taken care of in the site information base with an interface with the treat. By and by in case the customer visits a comparative site again, by then treat is moreover sent and web worker from the set aside information base pulls comparative tendencies and accommodates customer.

5. BASIC STEGANOGRAPHIC MODEL



As found in above picture, both the chief picture file(X) and mystery message (M) that should be covered are managed into a steganographic encoder as data. Steganographic Encoder work, f(X,M,K) inserts the conundrum message into a spread picture record by utilizing procedure like least essential piece encoding. The subsequent stego picture glances from an overall perspective equal to your spread picture record, with no unquestionable changes. These finishes the way toward encoding. To recover the riddle message, stego object is managed into Steganographic decoder. This paper will help you with actualizing picture steganography using Python. It will help you with forming a Python code to hide texts using a system called Least Significant Bit.

5.1Least Steganographic Model

We can portray a modernized picture as a limited game-plan of bleeding edge attributes, called pixels. Pixels are the smallest individual portion of a picture, holding respects that address the miracle of a given covering at a particular point. So we can consider a picture an association (or a two-dimensional gathering) of pixels which contains a fixed number of lines and zones.

Least Significant Bit (LSB) is a method wherein the last piece of every pixel is changed and dislodged with the mystery message's information bit From the above picture obviously, on the off chance that we change MSB it will largely affect the last worth however on the off chance that we change the LSB the effect on the last worth is negligible, in this way we utilize least critical piece steganography.

5.1.1How LSB Techniques Work

Each pixel contains three characteristics which are Red, Green, Blue, these characteristics run from 0 to 255, toward the day's end, they are 8-piece regards. We should take an instance of how this procedure capacities, expect you have to cover the message "howdy" into a 4x4 picture which has the going with pixel regards:
[(225, 12, 99), (155, 2, 50), (99, 51, 15), (15, 55, 22), (155, 61, 87), (63, 30, 17), (1, 55, 19), (99, 81, 66), (219, 77, 91), (69, 39, 50), (18, 200, 33), (25, 54, 190)]

Utilizing the ASCII Table, we can change over the puzzle message into decimal qualities and a brief timeframe later into equivalent: 0110100 0110101.Now, we reiterate over the pixel respects independently, coming about to changing over them to twofold, we supersede each most un-fundamental piece with that message bits continuously (for instance 225 is 11100001, we abrogate the last piece, the spot morally legitimized (1) with the basic information bit (0) thus on). This will essentially change the pixel respects by +1 or - 1 which isn't obvious in any way. The resulting pixel respects in the wake of performing LSBS is as appeared as follows
[(224, 13, 99), (154, 3, 50),(98, 50, 15),(15, 54, 23),(154, 61, 87),(63, 30, 17),(1, 55, 19),(99, 81, 66),(219, 77, 91),(69, 39, 50),(18, 200, 33),(25, 54, 190)]

6. TOOLS FOR IMAGE STEGANOGRAPHY

- Open Stego
- Quick Stego

7.DEVICES TO DISTINGUISH STEGANOGRAPHY

The crippling or expulsion of concealed data in pictures is subject to the picture handling strategies. For instance, with LSB strategies for embeddings information, basically packing the picture utilizing lossy pressure is sufficient to impair or eliminate the covered-up message. There are a few accessible steganographic identification apparatuses for example, Encase by Guidance Software Inc., I Look Investigator by Electronic Crimes Program, Washington DC, different MD5 hashing utilities, and so on

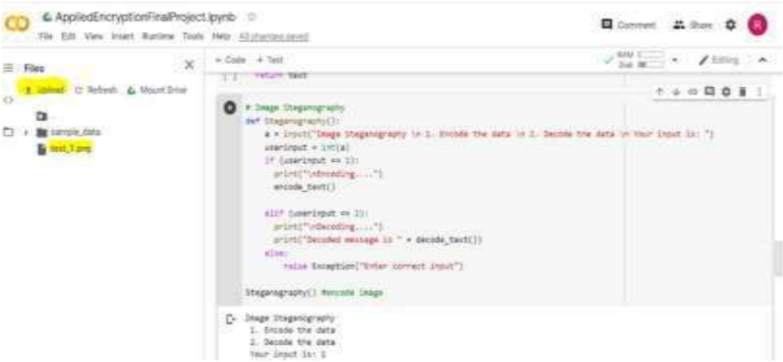
8.CORRELATION OF STEGANOGRAPHY AND CRYPTOGRAPHY

Steganography and cryptography are firmly related. Cryptography scrambles messages so it can't be perceived. Steganography on the other hand, shroud the message so there is no information on the presence of the message. With cryptography, examination is made between bits of the plaintext and segments of the code text. In steganography, examinations might be made between the cover-media, the stego-media, and potential bits of the message. The outcome in cryptography is the code text, while the outcome in steganography is the stego-media. The message in steganography may or then again may not be encoded. In the event that it is scrambled, at that point a cryptanalysis method is applied to remove the message.

9.MIX OF STEGANOGRAPHY AND CRYPTOGRAPHY

The individuals who look for a definitive in private correspondence can consolidate encryption and steganography. Encoded information is more hard to separate from normally happening marvels than plain content is in the transporter medium. There are a few devices by which we can scramble information prior to concealing it in the picked medium. In certain circumstances, sending an encoded message will over doubt while an undetectable message won't do as such. The two strategies can be consolidated to deliver better security of the message. In the event that, at the point when the steganography fizzles and the message can be identified, it is still of no utilization as it is scrambled utilizing cryptography methods.

10. CONCEALING TEXT IN IMAGE USING PYTHON


AppliedEncryptionFinalProject.ipynb
File Edit View Insert Runtime Tools Help All changes saved
Comment
Share
Files
Upload
Refresh
Mount Drive
sample_data
test_1.png
+ Code
+ Text
Editing

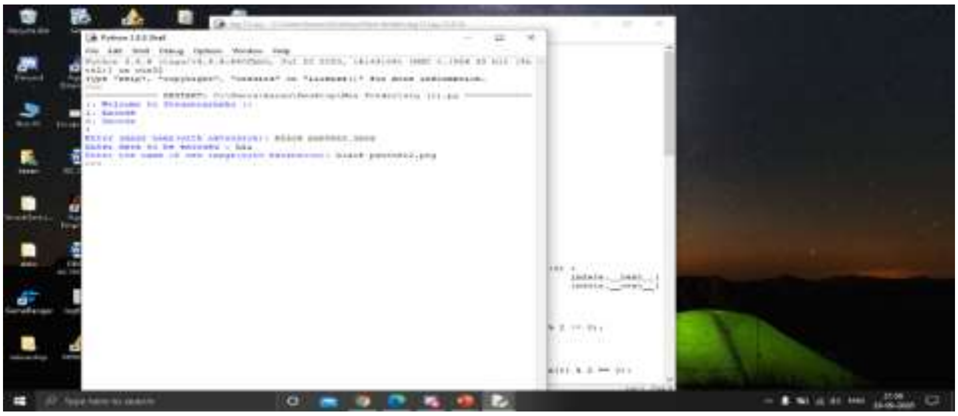
```
    return text
```

```
# Image Steganography
def Steganography():
    a = input("Image Steganography \n 1. Encode the data \n 2. Decode the data \n Your input is: ")
    userinput = int(a)
    if (userinput == 1):
      print("\nEncoding....")
      encode_text()

    elif (userinput == 2):
      print("\nDecoding....")
      print("Decoded message is " + decode_text())
    else:
        raise Exception("Enter correct input")

Steganography() #encode image
```

```
Image Steganography
 1. Encode the data
 2. Decode the data
 Your input is: 1
```

Import all the required python libraries.

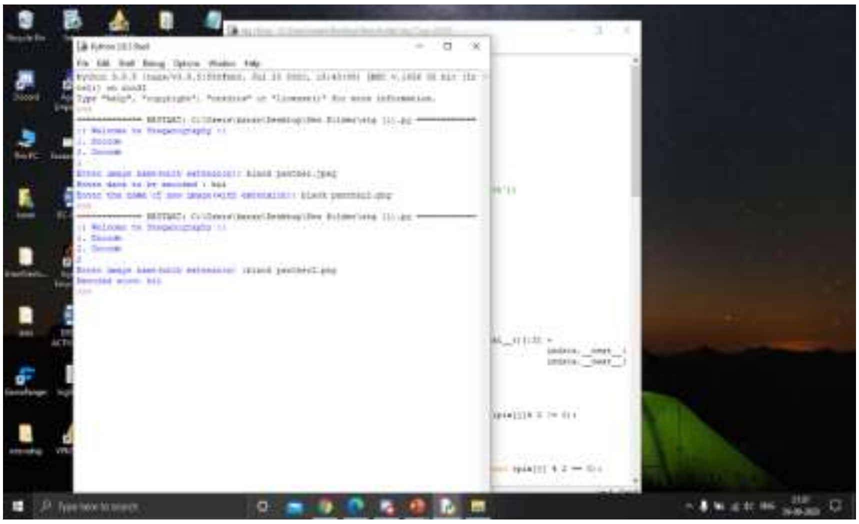
11.. ENCODING THE MESSAGE



```
[illegible]
Type "help", "copyright", "credits" or "license()" for more information.
>>>
==================== RESTART: [illegible] ====================
:: Welcome to Steganography ::
1. Encode
2. Decode
1
Enter image name(with extension): black panther.jpeg
Enter data to be encoded : hai
Enter the name of new image(with extension): black panther2.png
>>>
```

Fig -6 Encoding the Message

12. DECODING THE MESSAGE



```
[illegible]
Type "help", "copyright", "credits" or "license()" for more information.
>>>
==================== RESTART: [illegible] ====================
:: Welcome to Steganography ::
1. Encode
2. Decode
1
Enter image name(with extension): black panther.jpeg
Enter data to be encoded : hai
Enter the name of new image(with extension): black panther2.png
>>>
==================== RESTART: [illegible] ====================
:: Welcome to Steganography ::
1. Encode
2. Decode
2
Enter image name(with extension) :black panther2.png
Decoded word: hai
>>>
```

13.CONCLUSIONS

To conclude, This Paper Steganography using python which has been developed using Python. This paper helps users to hide data inside another image file. Which provides Easy implementation. Thus, the paper entitled above should include all the above-mentioned features and it is confirmed that it is up to the specifications entitled for the project.

13.1 Key features of this application

It can create another image file same as the original image file with different file name.

It provides:

-Fast encoding of data

-Fast decoding of data

-Easy and efficient user experience.

14.REFERENCES

[1]. https://securelist.com/steganography-in-contemporary-cyberattacks/79276/
[2]. https://www.tutorialspoint.com/image-based-steganography-using-python
[3]. https://www.tutorialspoint.com/python-image-based-steganography
[4]. https://www.edureka.co/blog/steganography-tutorial
[5]. https://www.techopedia.com/definition/4131/steganography
[6]. http://webtorials.com/main/eduweb/security/tutorial/steg/steg.pdf
[7]. https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-at443-steganography.pdf
[8]. http://eeweb.poly.edu/~yao/EE4414/memon_F05_v2.pdf
[9]. https://www.dreamincode.net/forums/topic/27950-steganography/
[10]. https://www.ijcaonline.org/archives/volume133/number9/23816-2016908016