

Image Steganography and Sending Private Data through Email Using Cloud Computing

Sai charan Salluri¹

¹Student, Computer Science Department, Jain University, Jaya Nagar, Bengaluru, India.

Corresponding Author: scsalluri@gmail.com

Abstract: - Steganography is a well-defined process of shielding a secret message i.e. information or data inside a larger one or comparable one in a form that one who is not intended could not know the ingredient of the hidden message or information. Even though related, Steganography should never be compared with Encryption, which is the process of encoding data or information in such a way that it can only be read by certain people —Steganography attempts to hide the existence or presence of data or information. The huge benefit of this steganography algorithm implemented in python is that it is simple and secure mechanism to transmit the stenographic image through email using the same platform. Because the stenographic message i.e. secret message is collaborated i.e. integrated disguised inside other nontoxic media sources, it is very severe to identify the data or information without having adequate knowledge of the existence of data and the appropriate encoding mechanism scheme. This project is hosted on Amazon Ec2 so that it can be accessed from any part of the world using the IP-address of the instance, thus giving this project an of advantage location independence.

Key Words: — *Image Steganography, Cloud Computing, Private Data, Python, Amazon Ec2.*

I. SCOPE OF THE PROJECT

The project has been completely built in python3 which is a modular programming language and using updated functions which won't be deprecated soon. Most of the GUI components used in the project are not platform dependent i.e. can work in any system where the IDE (integrated Development Kit) is similar and have all the packages installed. The modules used in this for GUI like PyQt5 and tkinter are very famous and can work in any platform. This project can be used as a go to for sending private data in day-to-day life without using any third-party application. [1]

The GUI of this project gives a feel-good and easy understanding of the whole process and are linked to one another in a jagged manner where the user gets all the information about the Host image and the amount of data that can be transmitted. It also provides a technique of embedding the contents of a text file directly into the picture without even user manually opening the file from his computer. This GUI application will save a copy of the stenographic image in the local system to ensure the data is never lost and can be used again if the email was unsuccessful.

This project can be used as a daily “ready to use” software for sending private data or other confidential information through Gmail without losing the confidentiality of the message [2]

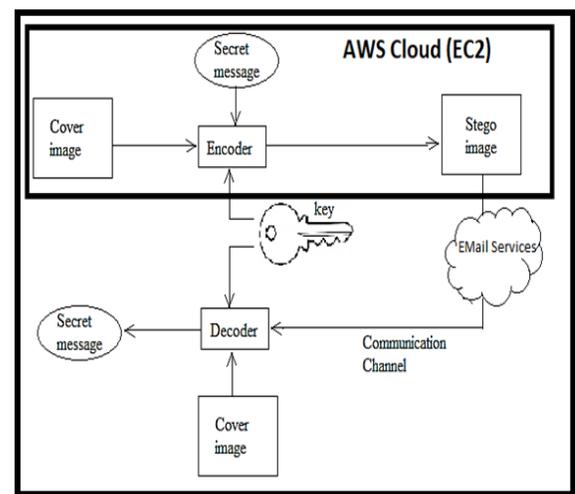


Fig.1. Architecture

II. ABOUT THE PROJECT

The algorithm shows an interest and slight modification toward the algorithm and method proposed by Data Embedding into Image Encryption using the Symmetric Key for RDH in Cloud Storage G. Preethi and N.P. Gopalan. Which was published in 2018 as well as uses modern programming language, and cloud computing techniques to improvise the working and more usable in modern day scenario.

This Project uses newer modules like PyQt5 and PIL instead of older modules, which have been deprecated in python 3.8,

and provides a better Graphical User Interface for easy understanding and user-friendly experience.

III. EXISTING SYSTEMS

In the existing systems, secret messages are stored and third party apps are used to transmit but it gives a problem to the unintended people who doesn't have any knowledge and also maintaining privacy is very difficult as of the intelligent of the hackers.[3] Already we have cryptography for transmitting secret data or information. Even though cryptography successfully transmits secret information, it will give a hint to the hackers and it affects unintended users. [4]

A. Drawbacks With The Existing System

Although there are many steganography applications but most of them lack in the one or more below features:

- No detailed information about the Host Media
- No details of amount of data can be send
- Inbuilt email service
- No Easy GUI implementation
- No line spacing Options for skipping pixels
- Cannot be Used on daily basis

IV. PROPOSED SYSTEM

My project is hosted on Amazon EC2 windows instance, which can be running all the time so that the project will be accessible from all over the globe as amazon charges very less money for providing such services, this will be a very inexpensive project. Sending Private Messages Using Image Steganography overcomes the factor and it gives a solution for sending secret formation without effecting unintended users and provides go to solution for sending private messages through steganography and built image services.

Steganography uses multimedia data as a covering medium i.e. Host medium (for covering secret information). By using steganography data (secret information) can shadowed with in Host Data (here data refers as multimedia data, In my case it is an image) and it can be sent anywhere using any email services which is built in the same application or else can be stored in the local system for later use without giving any suspicion to others.

A. Features Of Proposed System

- User friendly Graphical User interface
- Easy to Use
- Information about the Host image
- Displays Real-time data evaluation

- Inbuilt email service to send the stenographic image through mail
- Can be Used as a Daily go to send private messages through steganography
- Hosted on Cloud so can be accessed from any where
- Could be replicated easily using templates

V. SYSTEM IMPLEMENTATION

Using Amazon Web Services will be launch an EC2 instance where we can copy the code developed on local machine and run it using PyCharm IDE. As the installed EC2 instance will work as a normal windows server or windows machine there will no problem of installing any software and gives many advantages of free memory space and accessibility for anywhere in the world having good internet connectivity [5]

This project needs Python 3 and IDE like PyCharm to Run. Project is implemented in PyCharm IDE, so it can be run in any platform, which has this IDE. For hiding data with in a picture or any media we need to execute the sender side program by clicking encode button for extracting the hidden secret information or data we need to execute receiver side program by clicking the decode button after uploading the image. This steganography application will contain both sender side and receiver side programs. If a user wants to hide data or any sort of information, he can execute sender side program and if he wants to extract the secret data or information, he can use and execute the receiver side program and also after encoding he can directly send the image as an email attachment directly to anyone who he want to share the secret information

A. Hardware Requirement

- 1GB RAM minimum. (2 GB RAM recommended.)
- 1024x768 minimum screen resolution
- Processor: core 2 Duo or Higher Version
- 40 GB hard disk space.
- Mouse or any pointing device
- Internet Service for connecting to AWS

B. Software Requirement

- Python 2.4 or higher
- Microsoft Windows 10/8/7/Vista/2003/XP (incl. 64-bit)
- PyCharm IDE
- Remote Desktop File for connecting to AWS EC2 instance

VI. CONCLUSION

The project titled “Image Steganography and Sending Private Data Through Email Using Cloud Computing” can be used as a ready to go software for sharing sensitive data over the internet using google mail services which are embedded in the software itself. This project provides a major advantage of writing the secret message in the picture, which makes it, look like a normal image. But when decoded using steganography produces the hidden message and thus keeping the confidentiality safe from unauthorized users.

REFERENCES

- [1]. https://www.researchgate.net/publication/328610228/Cloud_Steganography-A_Review.
- [2]. <https://www.geeksforgeeks.org/image-steganography-in-cryptography>.
- [3]. <https://cyber/defense.sans.org/resources/papers/gsec/steganography-corporate-environment-106511>.
- [4]. http://www.epitomejournals.com/VolumeArticles/FullTextPDF/84_Research_Paper.pdf.
- [5]. https://www.academia.edu/39218070/A_Review_of_Various_Steganography_Techniques_in_Cloud_Computing.