**STEGANOGRAPHY**

**INTRODUCTION:**

Steganography is the practice of hiding a secret message inside of (or even on top of) something that is not secret. That something can be just about anything you want.

 These days, many examples of steganography involve embedding a secret piece of text inside of a picture. Or hiding a secret message or script inside of a Word or Excel document.

Steganography software allows both illicit and legitimate users to hide messages so that they will not be detected in transit. This article provides a brief history of steganography, discusses the current status in the computer age, and relates this to forensic, security, and legal issues. The paper concludes with recommendations for digital forensics investigators, IT staff, individual users, and other stakeholders.

In the current use of technology, digital information transactions often occur through cyberspace. Some things that are sometimes considered trivial internet users are about the security of data transmission.

**PURPOSE**

The purpose of steganography is to conceal and deceive.

Many people have used the internet in daily communication. The rise of internet data theft makes the security of data transmission becomes very importantThe purpose of steganography is covert communication to hide a message from a third party. This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication

steganography is a practice that enables secrecy – and deceit.

**PROBLEM STATEMENT**

The cryptographic algorithm is an important role in providing data security when transacting over the internet. Cryptography is a technique of randomizing messages so they can not be read directly

Advanced Encryption Standard (AES) is one of symmetric cryptography algorithms that can be implemented in various hardware and various software languages

with high imperceptibility value means embedded message increasingly can not be detected by human vision senses

The process is done by swapping the smallest bit size of the embed media with the message bit to be hidden.

i)

LSB is one of the most popular technique which is used for hiding the secret message. LSB hiding technique works as it hides the secret message directly in the least two significant bits in the image pixels, which affects the image resolution, due to this it reduces the image quality and make the image easy to attack.

Least Significant Bit hiding technique LSB is the most popular Steganography technique

LSB uses the image as carrier message because the image file is the most popular for this purpose because it easy to send during the communication between the sender and receiver. It uses the RGB color image as carrier message

**OBJECTIVE**

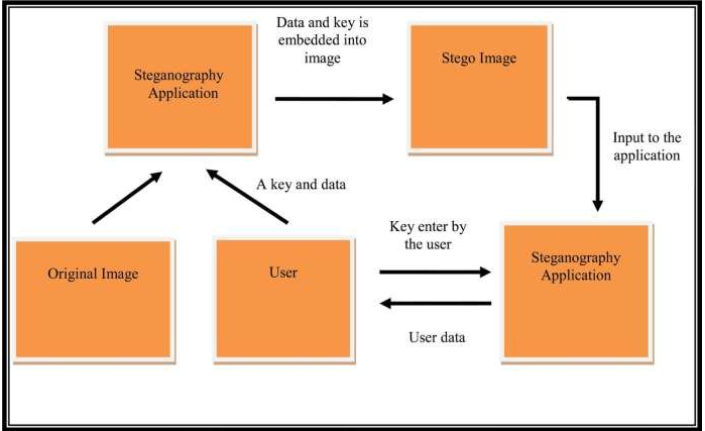
a. The of objectives steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

 b. This method featured security, capacity, and robustness, the three needed aspects of steganography that makes it useful in hidden exchange of information through text documents and establishing secret communication.

 c. Important files carrying confidential information can be in the server in and encrypted form No intruder can get any useful information from the original file during transmit.

 d. With the use of Steganography Corporation government and law enforcement agencies can communicate secretly.

**SYSTEM ARCHITECTURE**



**APPLICATION**

Steganography is applicable to, but not limited to, the following areas.

   1) Confidential communication and secret data storing

   2) Protection of data alteration

   3) Access control system for digital content distribution

   4) Media Database systems

There are many kinds of dedicated software applications available to facilitate steganography. Here is a partial list of the more well-known steganography applications:

* Image Steganography: This application is a [JavaScript](https://www.simplilearn.com/reasons-to-learn-javascript-article) tool used to hide images in other image files
* OpenStego: This program is an open-source steganography tool
* Xiao Steganography: Xiao hides secret files in WAV or BMP files
* Crypture: This application is a command-line tool used to conduct steganography
* NoClue: This application is an open-source tool that hides text information in both video and image carrier files
* Steganography Master: This app is an Android-based open-source tool that can hide text in an image and gives you a decoding tool to pull hidden text messages from image files. It supports multiple image formats (BMP, JPG, ICO, PNG)
* Steghide: Steghide is an application that hides data in different audio and image files, including JPEG, BMP, AU, and WAV

**ALGORITHM**

**i) Algorithm for embedding data inside image.**

Begin Input:

Cover\_Image, Secret\_Message, Secret\_Key;

Transfer Secret\_Message into Text\_File;

Zip Text\_File;

Convert Zip\_Text\_File to Binary\_Codes;

Convert Secret\_Key into Binary\_Codes;

Set BitsPerUnit to Zero;

Encode Message to Binary\_Codes;

Add by 2 unit for bitsPerUnit;

Output: Stego\_Image;

End

**ii)Algorithm for extracting data from stego image**

Begin Input:

Stego\_Image, Secret\_Key;

Compare Secret\_Key;

Calculate BitsPerUnit;

Decode All\_Binary\_Codes;

Shift by 2 unit for bitsPerUnit;

Convert Binary\_Codes to Text\_File;

Unzip Text\_File;

Output Secret\_Message;

End (reference : https://arxiv.org/ftp/arxiv/papers/1112/1112.2809.pdf)