Deep Learning In Steganography And Steganalysis

Supervisor

Asst. Prof. Dr.Bashar M.Nema

Submitted by

Rana Faris Najeeb & Asrss Safaa Ahmed

Out line

1. Abstract

- Deep learning is a subfield of machine learning which attempts to learn high-level abstractions in data by utilizing hierarchical architectures.
- Most deep learning methods use neural network architectures, which is why deep learning models are often referred to as deep neural networks.
- The term “deep” usually refers to the number of hidden layers in the neural network. Traditional neural networks only contain 2-3 hidden layers, while deep networks can have as many as 150.

Count …

- Convolutional Neural Networks (CNNs)

  is one of the most notable deep learning approaches where multiple layers are trained in a robust manner . Most deep learning methods use neural network architectures, which is why deep learning models are often referred to as deep neural networks.

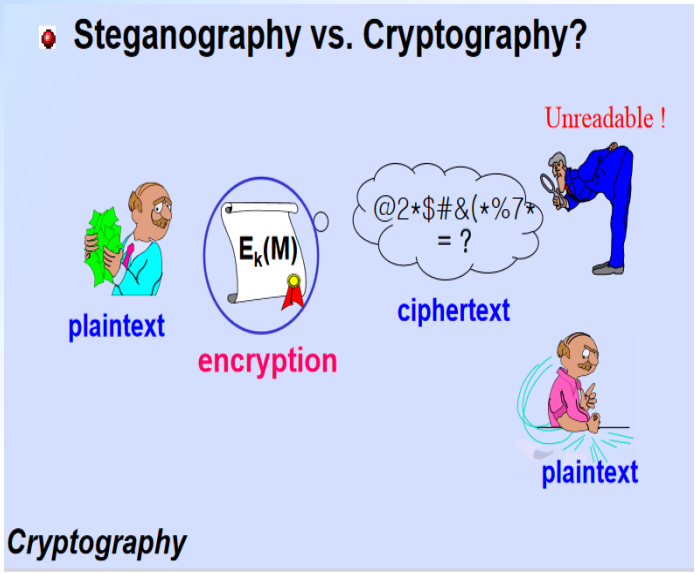
2. Introduction

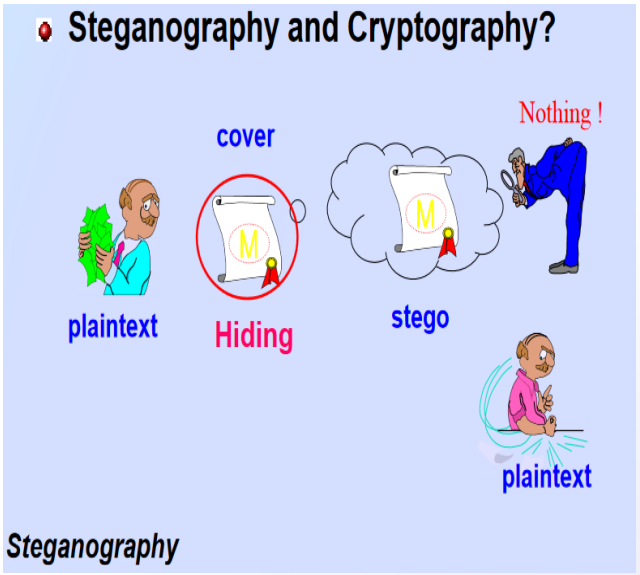
- With an advent of information era, more and more people utilize mobile devices for communication, working and creation. the personal privacy undergoes snooping, spreading, copyrighted ownerships, stolen works, etc. In solving such type of problems, the information hiding was given much attention for the protection of the copyright and privacy.

3. Theoretical Background

3.1 Steganography

Steganography, like cryptography?





3.2 Image Steganography Terminologies

Cover-Image: which represents the original image utilized as the carrier for the hidden information.

Stego-Image: following the embedding of the message in the cover image has been referred to as the stego-image.

Message: which represents the actual information utilized for hiding into the image. A message could be plaintext or anothers.

Stego-Key: which represents a key that is utilized to embed or extract messages from the stego-images and cover-images.

3.3 Types of Steganography

There are basically three types of steganographic protocols used. They are:

- Pure Steganography : which does not require the exchange of a cipher such as a stego-key.
- Secret Key Steganography : that requires the exchange of a secret key (stego-key) previous to communication.
- Public Key Steganography : that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly.

3.4 Steganography in the Digital Media

According to the cover object type, there is a number of the proper steganography approaches :-

- ✓ **Image Steganography:** the intensity levels of the pixel have been utilized for hiding information.
- ✓ **Network Steganography:-** the cover object like a network protocol, e.g., UDP, TCP, is utilized as a carrier.
- ✓ **Video Steganography**: which is an approach for hiding any information or file type in a digital video format.
- ✓ **Audio Steganography:** Audio steganography utilizes the digital audio format types, like MIDI, WAVE, etc.
- ✓ **Text Steganography:** the number of the white spaces, tabs, capital letters for achieving the task of information hiding

3.5 Steganography Techniques

- **Spatial Domain Methods** : in this method the secret data is embedded directly in the intensity of pixels such as (Least significant bit (LSB))
- **Spread Spectrum Technique:** In this method the secret data is spread over a wide frequency bandwidth.
- **Statistical Technique:** In the technique message is embedded by changing several properties of the cover.
- **Transform Domain Technique:** In this technique; the secret message is embedded in the transform or frequency domain of the cover.
- **Distortion Techniques:** In this technique the secret message is stored by distorting the signal.
- **Masking and Filtering:** These techniques hide information by marking an image. Steganography only hides the information whereas watermarks become a portion of the image.

3.6 Factors Affecting a Steganographic Method

1. Robustness
2. Imperceptibility
3. PSNR (Peak Signal to Noise Ratio)
4. MSE (Mean Square Error)
5. SNR (Signal to Noise Ratio)

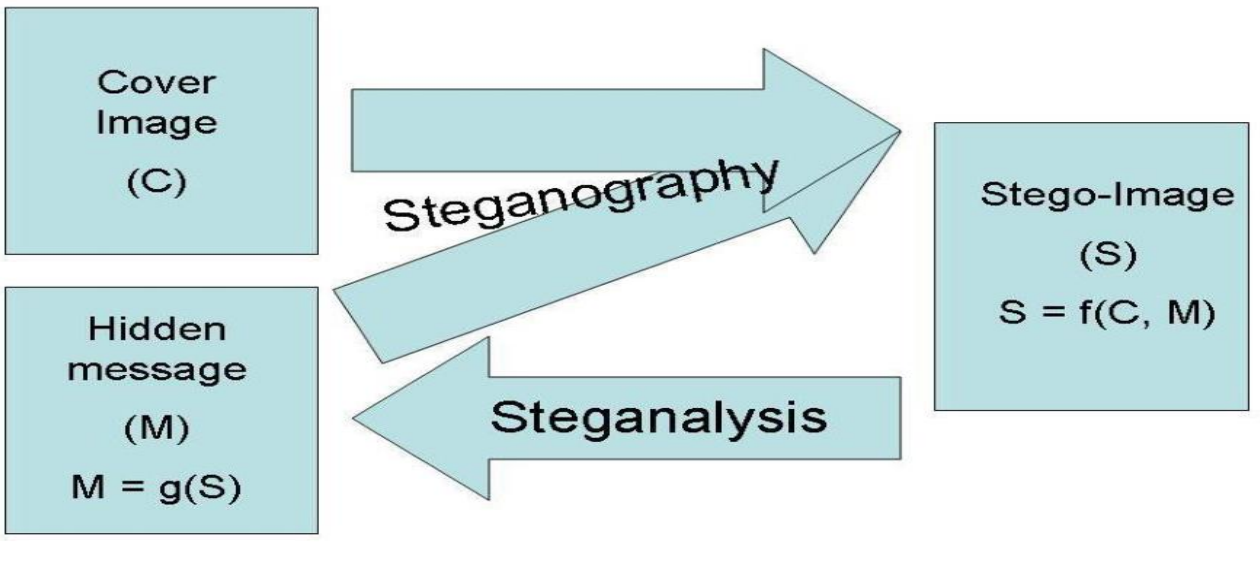
3.7 Application of Steganography

1. Confidential Communication and Secret Data Storing
2. Protection of Data alteration
3. Access Control System for Digital Content Distribution
4. E-Commerce & Media system
5. Database Systems.

3.8 Steganalysis

steganalysis can be classified into two major categories passive or active

1. **Passive steganalysis : -** tries to classify a cover medium as stego and identify the steganographic embedding algorithm.
2. **active steganalysis:-** additionally tries to estimate the embedded message length and ideally extract it from the



complete process of steganography and steganalysis

Count ….

Steganalysis can be classified into two broad categories based on prior information

- **A) specific/targeted steganalysis**

also called as targeted steganalysis, it is designed to attack one particular type of steganography algorithm.

- **B) blind/generic/universal steganalysis:**

The more general class of steganalysis techniques independently can be designed to work with any steganographic embedding algorithm, even an unknown algorithm.

4. Conclusion

- This study examines and presents deep learning-based picture information concealment methods from two perspectives: steganography and steganalysis. Although significant study has been done in these sectors, there are still certain issues that may be improved. Some steganography-based techniques, for example, are quite resilient, but their extraction approache still require being improved.

Thank you