Digital Forensics

SRN : PES1UG20CS825	NAME : PREM SAGAR J S	SEC : 'H'

Lab Assignment - 9

Explore how anti-forensic detection is done using Stegdetect,Write a report reflecting your understanding of the same.

- Anti-forensic detection helps investigators uncover hidden information and identify attempts to manipulate or hide data in digital forensics.

- Stegdetect is a tool commonly used in anti-forensic detection, and it's an open-source application that detects steganographic content in digital media.

- Stegdetect examines the least significant bits (LSBs) of image and audio files to find any changes that could indicate the presence of hidden information.

- This paper will explore stegdetect's functionalities and its uses in anti-forensic detection.

- Steganography is the practice of hiding information in another piece of data, such as an image or audio file, in a way that is hard to detect.

- Steganography has been used for both legal and illegal purposes, including spying, copyright infringement, and malware propagation.

- Stegdetect was developed to detect the presence of steganographic content in digital media by analyzing the LSBs of image and audio files.

- LSBs are the least significant bits of binary code, meaning they have the least impact on the overall value of a pixel or a sample in an audio file.

- Stegdetect analyzes the LSBs distribution in images or audio files to detect steganographic content. If the distribution is significantly different from an unmodified file, the suspect file is flagged as containing hidden information.

- Stegdetect can be used to detect steganography in various scenarios such as malware distribution, data exfiltration, message concealment, and evidence cover-up.

- Stegdetect is advantageous over other anti-forensic detection tools as it is open-source, detects steganography in both images and audio files, and is easy to use and integrate into automated forensic workflows.

- In conclusion, Stegdetect is a potent tool for detecting hidden information in digital media through LSBs distribution analysis.

==========**********==========