

Assignment 4

Name : Sonali Vedaraju

ID : 1002099198

Discuss how someone could find M or P, given (only) L.

Given only L it is difficult for the attacker to find the original message or carrier from the encoded image. The attacker can start from various bits and skip L bits to find meaningful data. Moreover, he/she will need to guess the file format of the encrypted message in order to get the hidden message correctly.

However, can try these:

Statistical Analysis:

Since every Lth bit is replaced by successive bits from M, there might be statistical irregularities in the distribution of bits within the carrier file P. Analysing the frequency of bit changes at intervals of L might reveal patterns that deviate from the expected distribution in unaltered data. With simple enhancement for L to change during the process, it becomes even more difficult to analyse.

File Size Analysis:

If the length of the carrier file P changes after the embedding process, it could be an indication that steganography has been used. Comparing the file sizes before and after the embedding process might reveal discrepancies. Hence, it enables the attacker to 'guess' that steganography has been used.

Azure link -

<https://steganography9198.azurewebsites.net>

.

Reference Links:

<https://www.geeksforgeeks.org/image-based-steganography-using-python/>

<https://stackoverflow.com/questions/74583881/audio-steganography-using-lsb-causing-noise-in-audio-with-hidden-message>