Contrast Enhancement Based Jpeg forensic detectability

ABSTRACT

Rapid advancement in digital image processing tools and software's has made it extremely simple to manipulate the digital images without leaving any footprints. It becomes a hot issue about the security and threat to society with increasing growth of social media. Image steganography hides secret information in an image called cover image so naturally that the other users cannot recognize the existence of information in the revealed image.

The project deals with the forensic department detecting compressed image even if it contains the presence of noise signal. The project investigates that the decoded hidden image information is a normal image or not. For detection two contrast enhancements based forensic algorithms via histogram peak/gap artifacts analysis. The normal and incorrectly decoded abnormal images have been trained using a deep neural network model and entropy features. The discrimination is processed with image patches since the information may be partially embedded in the cover image. The proposed approach discriminates and recovers the hidden image information automatically from a tremendously large number of steganography encoding methods

Reference:

- Kumar, G. Singh, A. Kansal and K. Singh, "Digital Image Forensic Approach to Counter the JPEG Anti-Forensic Attacks," in *IEEE Access*, vol. 9, pp. 4364-4375, 2021, doi: 10.1109/ACCESS.2020.3048246

SUBMITTED BY:-

Amal A S

Roll No:05

TVE18MCA006