Page: 1, paragraphs-1,2

Image manipulation has become very simple thanks to the availability of powerful image editing tools such as Photoshop and GIMP. As a result, developing forensic tools to determine the origin or verify the authenticity of a digital image is critical. These tools indicate whether an image has been modified and where the modification occurred. For digital image forensics, several methods have been developed. For example, forensic tools have been developed to detect copy-move and splicing attacks. Methods can also identify the manipulated region regardless of the manipulation type. Other tools can identify the digital image capture device used to capture the image. which can be used as the first step in many types of image forensics analysis. Digital cameras and scanners are roughly divided into two categories for capturing "real" digital images (not computer-generated images).

We are interested in forensics analysis of images captured by scanners in this paper. Unlike camera images, scanned images typically contain additional features created during the pre-scanning stage, such as noise patterns or artifacts produced by the devices that produce the "hard-copy" image or document. These scanner-independent features complicate scanner model identification. Many scanners also employ 1D "line" sensors, which differ from 2D "area" sensors found in cameras. Previous work in scanner classification and forensics has primarily focused on handcrafted feature extraction. They extract non-image content features such as sensor pattern noise, dust and scratches.

The goal is to classify an image based on the scanner model rather than the image's exact instance. Linear discriminant analysis (LDA) and support vector machine (SVM) are used to identify the scanner model using features that shows the noise patterns in the image. This method achieves high classification accuracy and is robust in the face of a variety of post-processing conditions (e.g. , contrast stretching and sharpening).