Abstract

In today's image driven world, we heavily rely on digital image data for various purposes – from entertainment to space research. Human brain is naturally accustomed to process visual contents at a greater speed; it is also called as the information currency. With sudden increase in image editing applications, one can easily make alteration in any image. Images shared using smart & mobile devices are hard to trust as an authentic one. It is a challenging task to cope up with ever increasing cases of alteration of images with malicious intentions. Altering the content of an image changes the semantics of the image and treated as digital image forgery. Digital image forgery is categorized into two categories – copy-move forgery and image splicing. Copy-move forgery is performed using a basic photo editing application where a part of an image is copied and pasted onto the same image. Image splicing is a composition technique in which cropped region of an image is pasted onto another image. For confirming the creditability of digital image without their prior knowledge, an image authentication method is required.

A lot of literature has been reported for the detection of forged image based on the intrinsic traces left by different component of digital camera during digital image acquisition process. It could be sensor-based noise inconsistent pattern, color filter array, lighting condition or even the metadata of the image. Due to the sensitive nature towards pixel value alteration such as brightness or contrast adjustment, post processing operations on the forged region is the major challenge in existing detection techniques. Existing copy-move forgery detection techniques suffers from the limitations of geometrical transformation of forged region and computation cost. Similarly, spliced image forgery detection techniques have shortcoming like single scope of application with single footprint, estimation of qualified sensor pattern and non-suitable features for

machine learning classification. Detection of forged scanned document is still an open research issue. These limitations are taken as motivation to navigate a path ahead in the direction of overcoming them. So, key objectives of the research are advancement is existing copy-move and spliced image forgery detection techniques, development of a generalized model for blind forgery detection and development of a model for forged scanned document detection. Thus, the problem statement can be defined as- Design and development of some digital image forgery detection techniques — copy-move, spliced image and forged scanned document centred— to address various challenges with existing image forgery detection methods.

The main work of this thesis is to study and implement existing forgery detection techniques, mentioning their merits and demerits with close analysis and proposing new methods. First, this thesis focuses on a comprehensive literature review on types of image forgery detection methods including types of forgery. Then, a comparative study is done of various copy-move forgery detection techniques (i.e. block-based, keypoint-based and data-driven) by mentioning the pros and cons of the same and some models are then constructed based on the mentioned criteria for copy-move forgery detection. Key-point based techniques are sensitive with post-processing operations such as brightness change or contrast adjustment while block-based approaches are not robust against geometrical transformation. So, a technique is developed using combination of both (keypoint and block-based). Except this, to reduce detection time, a multi-scale multi-stage deep learning model is proposed which is robust against geometrical transformation overcomes the challenges of post-processing operations. The key intention of the research is to cover the existing literature on image splicing detection techniques as well as their comparative study. Non-suited features and non-qualified sensor noise pattern are crucial provocations in image splicing detection techniques. A technique is developed to classify the image

into forged and authentic using combination of handcrafted features and machine learning classifier. To localize the forged region an inconsistent noise pattern-based technique is developed. A qualified noise pattern detects the inconsistent pattern between forged and authentic region of an image. Finally, the major endowment of the thesis is to design some of the efficient data-driven methods which locate the suspected region in an altered image or in a forged digital document whose type of forgery is not known. Due to the different characteristics of digital documents, techniques of digital image forgery detection don't work with forged digital documents. In this case, the most important challenge is the unavailability of publicly available dataset. Thus, a forged digital document dataset is also constructed with the model to detect them.

All the proposed models presented in this thesis are evaluated on multiple publicly available datasets and compared with state-of-the-art techniques. Experimental results of the proposed copy-move forgery detection techniques show that these techniques are not only efficient in detecting copy-move forged regions but also robust towards brightness, contrast change, noise addition, geometric transformations like scaling and rotation and multiple copy-move forgeries. The machine learning-based proposed spliced image forgery detection technique can discriminate the altered images from original images instantly. Whereas inconsistent noise pattern-based spliced image forgery detection technique can locate the forged region in a manipulated image. The developed blind forgery detection technique passed test cases of different synthetic forged images whose acquisition sources are different. Finally, the developed data-driven model for the detection of forged digital documents works on different post-processing operations as well as geometrical transformations of manipulated regions. This thesis also discusses the possible research direction in the area of digital image forgery detection.