# Chapter 11
# Advancements in Image Integrity Verification Techniques and Challenges in AI-Driven Forensics

**Mona Moussa**
https://orcid.org/0000-0002-3647-1993
*Electronics Research Institute, Egypt*

**Rasha Shoitan**
https://orcid.org/0000-0003-0372-4293
*Electronics Research Institute, Egypt*

## ABSTRACT

*In the internet era, images and videos face significant danger from criminals seeking to manipulate and conceal evidence of their crimes. The authenticity of image and video evidence cannot be guaranteed, making it challenging to consider them strong proof in a law court. The ongoing competition between researchers developing forgery detection tools and forgers creating more sophisticated manipulation techniques adds complexity to creating a universal tool for efficiently detecting various types of forgeries. Numerous approaches have been proposed to assess the authenticity of images; this chapter conducts a comprehensive literature review and comparative analysis of recent effective techniques designed to discover image forgeries. The emphasis is on addressing copy-move and splicing attacks frequently encountered in such scenarios. The chapter also identifies commonly used datasets and evaluation metrics in this field. The chapter also highlights existing challenges*

DOI: 10.4018/979-8-3373-0857-9.ch011

*and provides valuable insights into potential future directions for research in image forgery detection.*

## INTRODUCTION

With the rapid progress of consumer technologies like image editing tools and artificial intelligence, altering and fabricating digital images has become more accessible and cost-effective. While some image modifications are benign, such as improving visual appeal, others serve harmful objectives, like distorting facts to propagate misinformation about people, groups, or incidents, or even constructing false evidence for criminal defense. The proliferation of such deceptive images presents serious risks to legal systems, global markets, economic stability, and national security. Therefore, in recent years, the field of digital forensics, and specifically image forensics, has naturally shifted its focus to identifying deliberate modifications in digital images. Methods for identifying these alterations are broadly classified into active and passive techniques, as illustrated in figure 1. Active techniques involve embedding a watermark or signature into the original image immediately upon capture. The key challenge lies in designing an insertion method that is robust enough to withstand minor, unintended alterations such as noise or compression during transmission, while remaining sensitive to subtle, intentional manipulations introduced by human intervention. A significant drawback of active techniques is that they need prior knowledge of an image, which means that it is not applicable when dealing with images from unknown sources (V. Sharma et al., 2016). Additionally, given the vast number of images being captured daily, it becomes impractical to embed a watermark or signature in every single image. Consequently, there is a growing demand for methods capable of detecting image forgery in images from unknown sources. To address this need, passive detection methods have been developed as an alternative. Unlike active techniques, passive approaches do not rely on any prior information about the image. Instead, they work solely by analyzing the image's data, without requiring any external input. Passive forgery attacks can generally be categorized into image retouching, image splicing, and copy-move techniques. Specifically, the process of image retouching involves subtle modifications that enhance or reduce certain features of an image. This technique is widely used in fields such as magazines and film photography, where images are enhanced to improve their appearance. For instance, specific elements, like the removal of wrinkles, are adjusted to achieve the desired aesthetic outcome. While these modifications are typically intended for enhancement rather than deception, they still qualify as forgery because they compromise the authenticity of the original image (P. Sharma et al., 2023). In addition to retouching, image splicing is another preva-

# Security Framework for Smart Visual Sensor Networks

G. Suseelaand Y. Asnath Victy Phamila (2021). *Research Anthology on Artificial Intelligence Applications in Security (pp. 250-268).*
www.irma-international.org/chapter/security-framework-for-smart-visual-sensor-networks/270601