INNOVATION PARTNERSHIPS
UNIVERSITY OF MICHIGAN

Focal Stack Camera as Secure Imaging Device

TECHNOLOGY NUMBER: 2021-084

OVERVIEW

A built-in optical system with algorithms to make secure digital still images and videos

- Utilizes transparent detector planes to create focal focal-stack images
- Offers improved forgery detection that applies to various media types

BACKGROUND

While digital images are convenient for users because they are easy to take, store, and share, they are also susceptible to malicious manipulation. Advancements in deep learning has led to relatively easy reconfigurations of images and videos into high fidelity fakes. Methodologies for these manipulations include splicing new objects into the content, removing objects which were originally present in the image, and replacing one face with another. Faked images have been utilized to promote inaccurate news with the goals of fostering financial hoaxes or political propaganda. Altered images have even been submitted as pieces of evidence in criminal investigations.

Existing methods which are employed in an effort to prevent malicious image manipulation all function by influencing the software processing of an image after it has been obtained. In what is considered to be an active approach to dealing with this issue, semi-fragile watermarks are embedded in an image and are eliminated by malicious editing. The watermarking approach is robust is particularly effective in detecting resizing of an image, though it also alters the original content by its presence. A passive approach that is simple to implement relies on the use of imaging artifacts caused by lens distortion, color filtering, photo response non-uniformity (PRNU), and compression to perceive changes. The passive approach is limited because of its reliance on weak traces that are likely to be destroyed after compression or resizing of an image.

Technology ID

2021-084

Category

Hardware

Engineering & Physical Sciences

Inventor

Jeffrey Fessler
Theodore Norris
Zhaohui Zhong
Zhengyu Huang

Further information

Joohee Kim
jooheek@umich.edu

Learn more

So, despite existing machine learning algorithms used to detect image manipulation, a need remains for security systems built into the hardware of the camera that could facilitate forgery detection and prevention.

INNOVATION

Researchers have created a technology which combines a built-in optical system with algorithms to make secure digital still images and videos. The camera is modified by placing one or multiple transparent detector planes stacked along the optical axis between the complementary metal-oxide semiconductor (CMOS) chip and the lens of a camera. This system is therefore capable of capturing focal-stack images, at varying depths of a scene. The methodology of this approach therefore includes intake of a stack of images for a given scene, each of which is captured at a different focal plane by an imaging device. The stack of images can then be measured for self-consistency, which can then designate the existing image as authentic. Those images that are not self-consistent would be deemed manipulated. The innovation effectively makes it laborious to defocus blur signature across the focal stack, thereby dissuading those who would wish to tamper and forge the images. As such, this unique solution integrates hardware and software components to improve security in imaging.

ADDITIONAL INFORMATION

Patent Application

Number: 17/474,546

References

Huang, Zhenguy, Fessler, Jeffrey A, and Norris, Theodore B. , Focal stack camera: depth estimation performance comparison and design exploration. Opt. Continuum 1, 2030-2042 (2022). https://doi.org/10.1364/OPTCON.472819