TECHNOLOGY OFFER

Detection of image manipulation through a Novel, innovative method

During the last decades considerable progress has been made in the development of professional image editing software. As a negative side-effect, images have become more vulnerable to manipulation resulting in fake news and data. Currently, it is impossible to test the originality of a digital image without long lasting forensic analysis. Researchers at the University of Graz have developed a simple software solution that unveils image manipulations by means of an invisible code written on the image. This method reliably detects various forms of image manipulation and does not depend on access to the internet. Unlike state-of-the-art steganographic methods, this novel algorithm does not manipulate the least significant bit and is not based on invisible watermarks. The simplicity of the algorithm is striking and requires almost no computational effort.

BACKGROUND

The use of digital images, especially on social media, includes the risk of misuse of data and image manipulation. Fake images can easily be posted on social media because identification of image originality is difficult. A simple method that writes an invisible code on the image allows the identification of image manipulation later on. This is very useful for any camera company, because image originality can be checked through a simple app.

TECHNOLOGY

To enable the identification of fake images, an invisible code is written on original camera images by means of a novel algorithm. This code is generated right after shooting an image and gets lost after the manipulation of the image content or image size. This method makes use of the fact that the human eye has difficulties in discriminating small grey value differences. Implemented on a camera, this code can label an image to certify its originality by using a readout software. The technology used does not require connection to internet databases (blockchain, reference image stores).

ADVANTAGES

- This anti-fake algorithm can be used for a variety of cameras, e.g. smartphone and professional cameras
- It works faster than other protection methods
- It does not require internet connection to databases
- The readout app is very efficient and easy to use

WISSENS/ TRANSFER/ SÜD/

www.wtz-sued.at

KEYWORDS:
IMAGE PROTECTION
ANTI-FAKE ALGORITHM
FAKE IMAGES
FORENSIC IMAGE TOOL
STEGANOGRAPHY
SOCIAL MEDIA
SENSOR TECHNOLOGY
CAMERA TECHNOLOGIY
SMARTPHONE CAMERA
MOBILE PHONE CAMERA
CELL PHONE CAMERA

INVENTOR:
MANFRED HARTBAUER

COOPERATION OPTIONS:
LICENSING AGREEMENT
RESEARCH COOPERATION AGREEMENT

DEVELOPMENT STATUS:
DEMONSTRATOR SOFTWARE AVAILABLE

INTELLECTUAL PROPERTY:
SECRET KNOW-HOW

PROJECT NUMBER:
EM2018_12

CONTACT:

Gernot Faustmann
University of Graz
Research Management
Universitaetsplatz 3
8010 Graz
T: +43 316 380 3994
gernot.faustmann@uni-graz.at
www.uni-graz.at

UNI GRAZ