Abstract title **Imaging device identification and detection of image tampering**

Co-author **B. Zitova[1], F. Sroubek[1], J. Kamenicky[1], B. Mahdian[1], A. Novozamsky[1], S. Saic[1], A. Zita[1], Z. Sima[2], P. Svarc[2], J. Horinek[3].**
[1]Institute of Information Theory and Automation of the CAS, Department of Image Processing, Prague, Czech Republic.
[2]Institute of Criminalistics, Audia-video department, Prague, Czech Republic.
[3]National Drug Headquarters of the Criminal Police and Investigation Service of the Police of the Czech Republic, Informatics department, Prague, Czech Republic.

Abstract text

Current forensic analysis of digital photographs, videos, and corresponding scanning devices often represents an important part of criminal investigation. Imaging devices such as digital cameras, camcorders, or scanners are nowadays widely used, many criminal acts are captured by them, and, moreover, some of the criminal acts are even directly dependent on them, like for example children pornography or tax evasions. In our research we focused on an identification of imaging devices under investigation and on following verification of an originality of acquired images. The ability to uniquely identify or to exclude certain types or models of imaging devices as possible imaging device is very important for the very investigation process. The *Imaging Device Identification* provides suggestions about the manufacturer and the given model based on the analysis of sensor noise characteristics and on the image-related EXIF information, which reflects camera producer. The noise characteristics were chosen for their discriminability, stability, and accuracy even under real conditions.

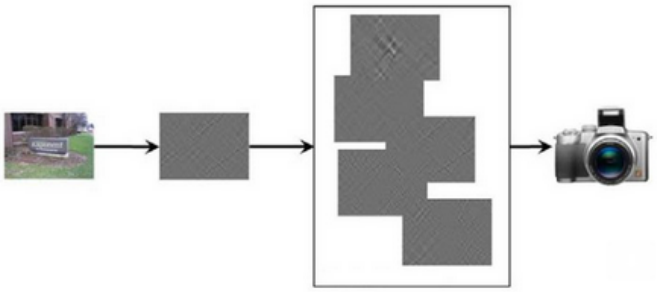
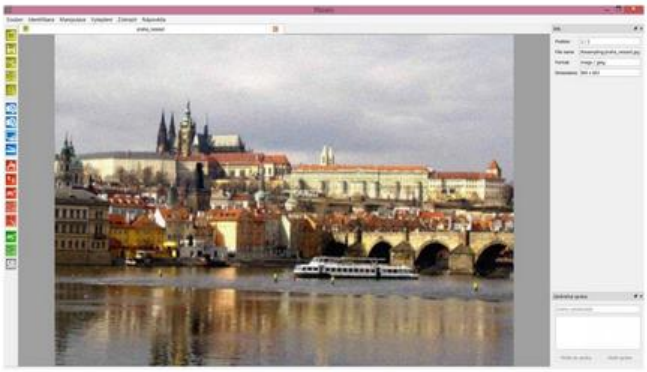


Figure: Noise characteristic for a camera identification.

The verification of the data acquisition source was proposed, too, in order to distinguish data from the camera, scanner and/or LCD panel. Proposed approach is based on the regularity of colors and patterns in images. In the second part of our work we paid attention to decision making if the data were intentionally manipulated. The tampering can serve for concealing unwanted image details, or even for creation of fictitious scenes. The *Analysis of Additional Changes* is devoted to the verification of such image data. The methodology is based on the image and video mathematical characteristics such as JPEG artifacts or traces after a image data interpolation, on estimated parameters of an image noise, on chromatic aberrations, and on moment-based descriptors.



Software PIZZARO

Software solution PIZZARO (http://pizzaro.utia.cas.cz) implements proposed solutions. Its development was funded by Ministry of the Interior of the Czech Republic and it was introduced to the Police of the Czech Republic. The PIZZARO development was realized in the tight cooperation of the Institute of Information Theory and Automation of the Czech Academy of Sciences and Institute of Criminalistics, Czech Republic.