Special Session

Forensics and Security of Physical Objects
organized by I. Tkachenko (LIRIS, CNRS, Université Lumière Lyon2), J. Picard (Scantrust) and S. Voloshynovskiy (University of Geneva)

Short description
Globalization and improvements in digital scanning and printing technologies have made counterfeiting more prolific and easier to perform than ever. According to a report commissioned by the International Chamber of Commerce, the entire global economy is on track to lose €3.7 trillion to counterfeiting and piracy with 5.4 million jobs at risk by 2022\(^1\). Counterfeiting also has a significant impact on our health and safety. According to the World Health Organization, up to half of malaria medications could be fake\(^2\), for a disease that kills around one million people globally.

Counterfeiting and forgery continues to proliferate partly due to the limitations of existing anti-counterfeiting technologies. Most of these technologies are either too easy to copy, too expensive to implement, too cumbersome to authenticate, or some combination therein. It has become trivial for counterfeiters to make visually perfect copies of physical products and the majority of the more secure methods for verifying authenticity cannot be used by consumers.

This special session aims at covering both forensics techniques (printer/scanner identification, 3D printer fingerprints, paper and ink identification) and security techniques (copy sensitive codes, natural and artificial randomness, security printing, printable digital watermarks, PUFs, etc.) for protection of physical objects.

Scope
The session scope is to explore and analyze novel techniques to protect, authenticate and ensure the integrity of physical objects such as packaging, branded products, or security documents. The section will focus on finding the links between forensics, image and signal processing, machine learning and cryptography and on presentation of the novel techniques to digitally assess the authenticity and integrity of physical items.

The session encourages contributions focused on novel techniques for physical object security, on making the existing protection solutions accessible to consumers on a large scale (e.g. by smartphone), and on the study of the security limits of existing techniques.

Paper submission deadline: July 14, 2021
Notification of paper acceptance: September 8, 2021
Camera-ready paper submission: October 6, 2021

All papers should be submitted via the regular WIFS 2021 submission service with the indication that the paper is submitted to the special session on “Forensics and Security of Physical Objects”.

---


\(^2\) [https://www.who.int/bulletin/volumes/88/4/10-020410/en/](https://www.who.int/bulletin/volumes/88/4/10-020410/en/)