Can printable unclonable codes be copied? Evaluating the performance of attacks and highlighting the role of the detector

Iuliia Tkachenko*[1]

[1]LIRIS, Lyon – Université Lumière-Lyon 2 – France

Résumé

Globalization and improvements in digital printing and digitalization technologies have made counterfeiting more prolific and easier to perform than ever. Counterfeits affects the world economics and human life as they are presented in majority of industries (from pharmaceutical, food and agricultural products to valuable documents). Counterfeiting and forgery continue to proliferate partly due to the limitations of existing anti-counterfeiting technologies. One of the promising solutions is the use of printable unclonable codes – small maximum entropy images, that take full advantage of information loss principle during printing and capturing process. These anti-counterfeiting solutions are successfully commercialized by several leading French and Swiss companies. However, recently the vulnerability of anti-counterfeiting solution based on these printable unclonable codes by deep learning attacks was shown. In short, the apparently simple question: "are printable unclonable codes secure against copy?", remains unanswered as of today. In this talk we will highlight the role played by the printable unclonable code detector and its different processing steps. Indeed, depending on the specific processing involved, the detection performance can widely outperform the printable unclonable code bit error rate which has been used as a reference metrics in the prior art.

*Intervenant