ABSTRACT

Steganography communicates a secret message as an innocuous looking object concealing the fact that something important is being communicated. Steganography is therefore more devious than cryptography, since when someone uses the latter, everyone knows that something is being hidden. Throughout history, steganography has been used by spies, agents, dissidents, and criminals. The oldest documented uses come from the old Greece at 5BC. With the advent of digitization, steganography has moved to the new media such as digital images, video, text, file systems, etc.

I will introduce the topic by talking about major breakthroughs in which I have participated, which have ultimately led to the most principled design of steganographic algorithms known to date, theoretically applicable to a diverse set of media such as images or sound. We will explain how error-correcting codes revolutionized the field. Since then, creating a new steganographic algorithm is equal to finding a good model of the noise. This is surprisingly difficult. Our first algorithm embracing this paradigm was broken in the first steganographic contest that we have organized. The rest of the talk would be devoted to the design of noise models by a combination of game theory and adversarial machine learning.