C17   The Application of Artificial Intelligence (AI) in Digital Forensic Science

Zeno J. Geradts, PhD*, Netherlands Forensic Institute, Den Haag, SH 2497 GB, NETHERLANDS

Learning Overview: The goal of this presentation is to learn from different possibilities in AI and know the limitations and possibilities.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by offering a brief statement on how AI impacts digital forensic science; however; validation is always needed.

AI tools that work like humans and learn from examples are often integrated into many different software tools, such as object detection tools, Automated Fingerprint Identification Systems (AFIS), face recognition, speaker recognition, author recognition, and many more. We see many different tools that are combined and used in pipelines to extract evidence from big data.

AI is included in many search engines and many products, and we are used to having them. Now, smart phones often include much AI for recognizing the user and predicting the information someone is interested in. Speech recognition works well enough to use for searching the internet. People are sometimes not aware that their digital devices, such as tablets and smart phones, are listening to their conversation if they have not turned the privacy modes on. Later, the user might get advertisements related to some words they were discussing, such as, for example, a vacation to Corsica if they were discussing that part of the world. In criminal settings, using certain phrases may later be used as supporting evidence in court.

For facial comparison, it is well known that bias exists, depending on the training sets. There are cities, such as San Francisco, that abandoned the use of this technology by the government due to bias and other privacy concerns. However, since facial comparison algorithms have proven to be much better, and in many cases outperform humans, the use of an algorithm to assist the forensic scientist is used more often. Sometimes, we have patterns, such as the Photo Response Uniformity (PRNU) to identify cameras, that a user cannot really see, and an algorithm can compare better. In practice, we see that AI is used to make faces that never existed, based on training material, such as the deep fakes.

For image and video manipulation detection, more algorithms are developed that also use deep learning techniques to detect the manipulation. It is very important that we can explain in court how these algorithms work, and that the results are validated. Also, we need to be aware that once a method for detection has been published, it is possible to attack the detection method. For this reason, it is necessary to perform continuing research on the application of methods in AI, without seeing it as a complete black box. The reproducibility of results with AI is another issue that should be addressed, since based on the starting point of a dataset, different results may be obtained.

AI, Neural Networks, Digital Forensic Science