AI for Digital Forensics

The field of Forensics is moving toward its third revolution in its short history. The first revolution was under J. Edgar Hoover who brought science into the field of forensics and is responsible for the advance of criminal justice as of today. The second revolution saw the joining of computers in the mainstream and formed a subdomain of digital forensics. We are now moving rapidly towards Artificial Intelligence(AI) in this new age of Big Data and IoT (Internet of Things)

Digital forensics has been handling large amounts of complex data requiring intelligent analysis. Hence artificial intelligence is the precise route for the future of digital forensics. Artificial intelligence is a new and modern area of computer science that is used to solve computationally complex problems in a short time frame.

The ultimate goal of artificial intelligence is to create a machine that imitates the human behavior of analyzing and understanding to make sound decisions. This is done by implementing various learning algorithms that help in making a sketch of what a human brain learns. AI can be said as a new toolbox helping forensics teams and solving cybercrimes.

Combining AI with digital forensics saves important time and expense by introducing automation. It also helps investigators detect malicious and suspicious activity in large and unstructured chunks of data scattered in social and wired networks and web or cloud storage. It gives the investigating team a more dynamic approach rather than rule-based testing. AI helps get rid of enormous information silos that continue on building and helps release the burden on the investigation teams to concentrate more on other possible cases of fraud and crime. Forensic investigators can get an edge over the investigation by using cognitive analytics which is self-learning and can analyze a huge amount of data dynamically and patterns can be recognized from it.

One such example of AI helping in cyber investigations is MultiAgent Digital Investigation toolKit (MADIK). MADIK consists of many Intelligent Software Agents (ISA) which help in performing many different analyses on the evidence. ISA interacts with the evidence, perceiving, and analyzing data autonomously to reach a final goal. MADIK is a Multi Agent System (MAS) comprising of many such ISAs working together in harmony to reach a defined individual or a group goal.

When a case is presented in a court, the judge should be able to understand the broad work done by AI and feel comfortable with its increasing role in the area of digital forensics. Digital forensic investigators using machine learning is the latest trend for seizing the potential of AI in forensics. Behavioral analytics is also used for profiling, modeling, and prediction of cybercrimes. Human decisions on complex cases are trackable and debatable, hence when using an AI-based tool, it is imperative to generate logs so that its outcomes are open and can be fully contested.

It would be fair to say that we are still in the basic stages of digital forensics using AI. But there is no contest to the fact that the age of AI is here and has changed the game to a whole new paradigm. Hence Digital Forensics stands on the way to transform itself into a whole new better self.

An Executive Summary by
Saket Thombre