AI ON DIGITAL FORENSICS

Artificial Intelligence (AI) is an important and well-established area of modern computer science that can often provide a means of tackling computationally large or complex problems in a realistic period. Digital forensics is an area that is becoming increasingly important in computing and often requires the intelligent analysis of large amounts of complex data. It would therefore seem that AI is an ideal approach to deal with many of the problems that currently exist in digital forensics.

Digital Forensics

According to the US-CERT forensics publication, *"*Digital forensics *is the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way thast is admissible as evidence whether during an investigation inside any organization or in a court of law."*

Artificial Intelligence

Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. The term may also be applied to any machine that exhibits traits associated with a human mind such as learning and problem solving.

The ideal characteristic of artificial intelligence is its ability to rationalize and take actions that have the best chance of achieving a specific goal.

CONTRIBUTION OF AI IN DIGITAL FORENSICS

Algorithms already play a significant role in helping digital forensics investigators analyze the vast amount of data that is created by mobile devices and stored on the cloud. Like many industries, demand outstrips supply when it comes to qualified, trained professionals who can sift through the backlog of digital forensics data relevant to modern criminal cases. Artificial Intelligence (AI) can help automate some processes and more quickly flag content or insights that would otherwise take investigators longer to uncover.

It's a bit like the show *Mindhunter* on Netflix, which tells the story of the first psychological profiling that helped coin the term "serial killer" and establish a new methodology for tracking criminals and identifying behavioral patterns early on. AI is another tool in the toolbox that is helping law enforcement agencies (and corporate in-house investigators) comb through the available data for insights—digital needles in the proverbial haystack.

AI functions can help with spotting and identifying elements in photos and videos, observing commonalities in communication, location, and times, and based on history, make educated guesses about where and when the next incident or crime might occur.

That being said, there is a trust factor to overcome with AI in digital evidence in criminal investigations. When evidence in a case is presented, the attorneys, judges, and jury members must grasp the broad concept of artificial intelligence in order to accept and feel comfortable with it's growing role in digital forensics and in many modern criminal investigations. Just human logic on complex decisions can be traced back and debated on any particular issue, it's imperative that AI functions have logs and so its conclusions are transparent and can be fully litigated.

And all of that is to say that human beings will still have a role in criminal investigations. AI is a tool, but it's not an investigator. We're far away from that, if we ever get there at all. So while it's important to understand and harness this tool, it's equally not to conflate AI as analogous to an investigator.

SOME OF AI TECHNIQUES THAT CAN HELP IN DIGITAL FORENSICS

Cases

Cases Case Based Reasoners (CBRs) are a type of (normally) symbolic AI that are an attempt to avoid some of the problems associated with symbolic rule based systems such as expert systems. CBRs are based on well understood notions from psychology on how domain experts themselves represent information.Most domain experts rely heavily on their past experiences, and when faced with a problem, will attempt to match the problem to one they have experienced before. Only when an expert has exhausted all possible similar cases in their experience do they use first principles to attempt to find a solution to the problem.

A CBR system works in a similar fashion, in that a large collection of cases (and in digital forensics, the resultant actions) is obtained, and a metric is used to match the current situation with one found in the case base. If a perfect match is found, then the action carried out in the initial case is applied to the existing situation. If no perfect match is found, but a match is found that is deemed to be close enough, then the system may attempt to adapt the action of the matched case to the current situation using what are called 'repair' rules. CBR systems have the advantage of approaching a problem in a way that is familiar to the expert, can cope with large amounts of data, and can deal with situations that have not previously been encountered. They address in part the ability to explain the reasoning process, because the reasoning can be inspected. This, however, means that the user might rely very heavily on the quality of the cases in the case base, together with a good coverage of the possible scenarios. CBRs are also limited, in that although they can help guide the process of the investigation, they are perhaps ill suited to helping to automate the lower level activities (such as "find all pictures with naked people in them").

Pattern Recognition

A type of AI known as pattern recognition best handles identifying specific types or clusters of data in an investigation. The type of pattern recognition that people are most familiar with is perhaps image recognition, where the software attempts to identify parts of a picture. Other forms of pattern and image recognition also exist, such as detecting a pattern in an e-mail message, which indicates SPAM, or a pattern in a disk image that might indicate it is part of a sound file. Many of the techniques used rely very heavily on statistics or probabilistic reasoning or both. The more complex and accurate forms of image recognition that might be used to locate certain types of picture rely on an understanding of how the human perceptual system works. However, at present these have a high rate of false positives or false negatives (depending on where the thresholds are set) as well as being very computationally intensive.

Pattern recognition systems are essentially classifiers – that is they answer the question: is this piece of data a member of the class X, where X is the type of data the user is interested in. In order to work successfully, pattern recognition techniques have therefore to try to match against

all possible pieces of data (or as near as is computationally feasible) which can involve a large amount of matches, and the patterns have to have sufficient generality to match all positive matches but sufficient specificity to not match any of the negative examples. In practice, this is often very hard to achieve, although Machine Learning techniques (for which see below) can help with the generality or specificity problem by allowing patterns to adapt, and in the case of certain systems, such as Artificial Neural Nets or decisions trees, can be used to learn the initial patterns.

Knowledge Discovery

Knowledge discovery is another field of AI that might have benefit in the forensic arena is Data Mining and Knowledge Discovery in Databases (Datasets). Although these terms technically refer to different things, the two terms are colloquially used interchangeably to refer to process of finding useful information in a large collection (normally sparse) of data. Data Mining/Knowledge Discovery in Databases (DM/KDD) is not a single technique but is a mixture of AI, statistical analysis and probabilistic techniques used together in an integrated manner to analyse large collections of data. It can be viewed as a form of pattern recognition, but with a few significant differences.

First, the sheer size of the data (in some cases petabytes) means that more computationally intensive techniques cannot be effectively used, therefore any AI technique involving the use of a complex knowledge representation is unlikely to be used for DM/KDD. Similarly, background knowledge about the domain may also not be used, or may only be used in a limited fashion.

Secondly, DM/KDD is often directed by the user. Technically this process is a form of Exploratory Data Analysis (EDA) where the user asks the system to, for instance, highlight files with characteristic X, and the system uses Data Visualisation (DV) to highlight information and potential relationships to the user. This is particularly useful, because the human perceptual system has the ability to distinguish patterns in extremely complex data – even in data with a large number of attributes16 – if the data can be represented properly. Care does, however, have to be taken, because the human perceptual system can find patterns that do not, in reality, exist.

Thirdly, DM/KDD has the concept of an interestingness measure (often called a J measure) that helps to decide whether there are any meaningful patterns in the data. This helps avoid the situation where a DM/KDD system ‘discovers’ the extremely obvious, but extremely unhelpful fact, such as that you only ever find female patients in the maternity ward of a hospital.

It is extremely likely then that, given the increase in quantities of data, the forensics community will have to rely on DM/KDD techniques to help with the initial assessment. To date they are the best AI method for dealing with large quantities of data, but they are also potentially the most likely to miss relevant pieces of information, because the reasoning processes do not normally use the background knowledge or complex reasoning of more complex AI approaches.

Adaptation

Adaptation A system that has a fixed knowledge source is unlikely to be able to cope well with the change in pace in computer technology, and therefore it is likely that some measure of adaptability will be required for any long-term forensic system. The branch of AI that deals with the ability of the software of a system to adapt is called Machine Learning (ML). From the point of view of interest in the applicability to digital forensics, ML techniques can be divided into two: ones that use ML as a method of trying to refine the knowledge source to keep it current (the refiners), and those who use ML to gather the initial knowledge (the learners). There are, of course, techniques which combine both approaches, but they can be thought of as a subset of the learners. Each type can in turn be divided into supervised (a human, called an oracle, gives the correct answer) and unsupervised (the system is left to find out its own answers).

CONCLUSION

The use of AI in digital forensics is still at a very early stage, but it does have a lot to offer the digital forensics community. In the short term, it is likely that it can be immediately effective by the use of more complex pattern recognition and data mining techniques, as discussed here However, for digital forensics to take full advantage of what AI has to offer, more work is necessary.

First, a suitable ontology must be produced for digital forensics, so that it is easy to record, reason about and exchange information about the evidence and processes used. This will help, both in terms of automating the digital forensic investigation and in terms of helping to record best practice in digital forensics.

Secondly, this ontology needs to be used to annotate suitable cases that can be shared with both digital forensics experts and AI experts. This collection of cases can provide help in bench marking both people and computer systems as well as opening up the opportunities for mainstream AI experts to help advance the use of AI in digital forensics.