Deep learning, a key technology behind IDEMIA's algorithms

By Stephane Gentric - IDEMIA's Global R&D Manager

ACCESS CONTROL
IDENTITY
TRAVEL
PUBLIC SECURITY

POSTED ON 07.26.21

We recently interviewed IDEMIA's Global R&D Manager, Stephane Gentric, to find out what deep learning is and how it works. It was interesting to understand the intricacies behind the innovative technology that teaches machines to 'think'.

Hello Stephane, thank you for taking the time to speak with us. Let's start with the first question, could you explain what deep learning is?

Deep learning is a subdomain of AI, based on Deep Neural Networks (DNN) with representation learning. It teaches machines to do what comes naturally to humans: learn by example.
Deep learning is the key technology behind many innovations such as video analytics. It can locate and recognize specific elements in video footage such as pedestrians, luggage, or even a facemask on a person. Instead of using task-specific algorithms it learns from representative examples—in order to do this efficiently the deep learning algorithms need to be provided with lots of data.

Where does IDEMIA obtain the data to train its deep learning algorithms?

Our data is obtained using three different methods. We have many clients who are willing to let us use their data to train our algorithms; in compliance with local and international privacy regulations, of course. We also frequently hold internal campaigns at IDEMIA offices around the globe, where our employees allow us to use their biometrics. This method allows us to gather data over the years, which is very important when training deep learning algorithms.

Last but not least, we create synthetic images. Using a Generative Adversarial Network (GAN), we have been able to create synthetic data using a real database. The synthetic data is similar to the real database, but it is in actual fact, completely fictional. We can, for example, generate qualitative synthetic facial images from different angles or fingerprints that do not belong to anyone. Not many companies are able to do this well, and this is one of the factors that differentiates us from other biometric companies.

In order to test the efficiency of our biometric algorithms, clients regularly ask us to share data with them. In compliance with GDPR regulations, we do not share the data of real people, so we share our synthetic data. Although synthetic images are not yet able to fully and accurately capture all the possible variations of a face—like aging or wearing makeup—they are a very good alternative that can be used on many occasions such as integration testing at full scale.

How do IDEMIA's deep learning solutions adapt to client needs?

Our clients are based around the world. Each client has specific technological needs and requirements. Some may need to have DNN deployed in the cloud, in an embedded platform, in an eGate or a central server. Our DNN takes available memory and computing power into account, enabling it to be deployed anywhere. Our systems are versatile from the get-go. When creating a DNN, we explore diverse network depths and sizes, including recent architectures such as ResNet, DensNet or attention-based networks.

During the learning process we minimize costs by working on several areas simultaneously. This allows us not only to improve the performance of our deep learning algorithms, but also to incorporate other topics such as fairness.

Can the efficiency of IDEMIA's biometric algorithms be measured?

We have been in the biometrics industry for several decades now. Our technologies have been rigorously tried and tested. They are trusted by our clients, who are proof that our algorithms work not just in test settings but in real-life situations on a daily basis.

That being said, the efficiency of biometric algorithms can be measured. Many of our clients will test our deep learning solutions before implementing them locally. They need to be sure that they will work the way they expect them to. Client satisfaction is of the utmost importance for IDEMIA.

There are also public benchmarking/testing organizations such as the National Institute of Standards and Technology (NIST) who test companies' biometric algorithms by measuring their efficiency. They will then publish the results—making them public for everyone to see. The company's expertise, experience, and know-how is public knowledge, so you could say our reputation precedes us. For many years, IDEMIA has participated in NIST benchmark testing for three biometrics: iris, face, and fingerprints. We are proud to say that we have always ranked in the top for these biometric benchmarks. Our facial recognition 1:N algorithm achieved best results for accuracy among 75 tested systems and 281 entrants during the 2021 Face Recognition Vendor Test.

How does IDEMIA maintain its position as market leader with its deep learning solutions?

We have an experienced R&D team dispatched around the globe that is an early adopter of cutting-edge techniques. The team has been developing new methods and researching deep learning for many years. In France, we have one of the biggest R&D teams in a corporate setting. We also work closely and have partnerships with scientific research associations. Many members of the French team give lectures on deep learning at universities in France. In addition, there are many PhD students in subjects related to machine learning across our French teams.

How does IDEMIA's R&D team come up with new deep learning solutions?

We work hand-in-hand with the different business units in order to understand client needs. We take their roadmaps into account to ensure that there is a direct link between the innovations we are working on, and what our clients need

in the field—who better to guide us than the product managers who are in contact with our clients on a regular basis?

We also work with the Center of Excellence Terminals and Equipment when we are developing a new sensor. When building a sensor for an access control door or for an airport eGate, the software is just as important as the hardware, and both are developed at the same time.

What was the impact of Covid-19 on IDEMIA's biometric algorithms?

We have frequent requests for new solutions—the pandemic was a perfect example of how IDEMIA hits the ground running. We had to adapt very quickly. As soon as the pandemic hit China, we started developing algorithms that were able to detect whether or not a person is wearing a face mask. We also started working on algorithms that can recognize a person (1:1 verification) wearing a face mask. We recently won a US rally organized by the Department of Homeland Security for this topic.

Additionally, we developed deep learning algorithms that can measure crowd density and the distance between people in public areas.

What is the future of deep learning and how do you see the techniques evolving?

There are a few subjects. First, there is perpetual need for better image and video processing technology. We strive to improve our existing algorithms as this will create more use cases for our clients. The technology used in video analytics is now at the point where it can automatically see inside cars to detect whether or not drivers are wearing their seatbelts, or if they are using their phones while driving. We can also detect motorcyclists who are not wearing helmets. These advanced technologies can help deter reckless behavior to strengthen the safety and security of drivers, passengers, and pedestrians.

Second, we work very hard to produce deep learning solutions that are fair and unbiased to everyone regardless of their age, ethnicity, or gender. However, this is not an easy process. Biases mainly come from training databases, which is why we make sure that our databases contain a variety of images of the same element in various acquisition conditions. For road safety, we train our algorithms with daytime and nighttime images. We also use pictures of the different weather conditions to ensure that our technology is effective in all environments. Today, we are proud to say that our biometric algorithms have reached such a high level of efficiency that biases can no longer be measured—there are not many biometric companies that can make such a bold statement and back the claim up.

And finally, more and more people want to know and understand how deep learning algorithms come to a certain conclusion. There is an increase in demand for the explainability of algorithms. This is a huge challenge for the industry because there is no straightforward answer and explaining why the deep learning technology made a certain decision is not as easy as one might think.

In the future, when we provide solutions to governments, some will have a legal obligation to explain why the algorithm came to the decision it did, which is not the case with deep learning algorithms today. DNN are very efficient, but they are not able to directly explain why they came to a particular decision.

How is deep learning/machine learning compliant with GDPR?

We have been working with the Commission Nationale Informatique & Libertés, the French data protection agency, for a very long time and have integrated GDPR into our technology. In addition, all data that we collect is done in adherence with local laws and regulations.

We are currently working on a family of algorithms for our upcoming video analytics technology. Using these deep learning algorithms, we will be able to anonymize people who are not related to the case being conducted. The faces of all people not related to the case will automatically and instantly be blurred to keep their identity completely confidential from the operators using the video analytics system.

In another example, when someone is trying to use an access control system, only the biometric data of the person requesting access will be divulged while the identity and biometric data of everyone in the background will be blurred automatically.

And finally, what does the future have in store for IDEMIA?

We have been, and always will be, dedicated to delivering secure and efficient client-centric solutions. Not only do we focus on the continuous improvement of our existing technology, but also on the creation of new biometric solutions.

Furthermore, we will ensure that our biometric algorithms continue to be as fair and unbiased as possible. We are working toward the clarification and explainability of our algorithms so that when needed in the future, our clients will be able to explain why an algorithm came to a certain conclusion.

The goal of our deep learning solutions is to help our clients ensure the safety and security of their citizens while respecting the fundamental right to privacy.