FACE RECOGNITION PROBLEMS FOR ARTIFICIAL INTELLIGENCE IN CASE WITH SOCIAL MEDIAS

Логвінова К.В.
Науковий керівник – к.т.н., ст. викл. Дейнеко А.О.
Харківський національний університет радіоелектроніки
(61166, Харків, пр.Науки,14, каф. штучного інтелекту, тел. (057) 702-13-37)
e-mail: kateryna.lohvinova@nure.ua

Nowadays, a certain kind of experience in the era of information technology and information technology, the problem of creating "smart" technology is especially urgent. On the "smart" technologies on the current day, you can rozumiti cars with programs of any complexity, all kinds of pralny machines, especially the robbery mode before the robots, which can make pictures and cherubs by co-workers.

In machine learning, the results can be biased or inaccurate based on the volume and type of training data used. That's probably because the historic pool of data used to train the algorithms included more men than women.

The idea was to give physical stores demographic information that could guide how they market to individual customers. It's something that could give them a competitive edge against online retailers such as Amazon, that have been leveraging customer data all along.

But using cameras to capture photos of your customers in a way they may not even notice seems like it could be crossing that line between cool technology and creepy technology. Is it too invasive? Beyond that, there could be other problems, too. What if the software misidentifies a man as a woman and offers him a discount on feminine hygiene products? What are the consequences?

The studies say that these algorithms are best at identifying lighter-skinned men. Their performance isn't as good when identifying women or darker-skinned people. The study also notes that some vendors improved their algorithms after these results were pointed out to them. Amazon's response

By adding more data or data sources to the pool used to train the algorithm, vendors may have improved the accuracy of their AI facial recognition systems.

The retail systems on display at NRF demonstrated how that works. For instance, in terms of gender, these systems may decide that someone is male. But they will also provide a confidence score, essentially saying that they are 67% (or some other percentage) certain that the person is male. Retailers have already set the level of confidence score they are willing to accept. So if someone is deduced to be male with a 67% confidence score and the retailer has set the threshold level at 60%, the customer will see the offer customized for a man. If the retailer sets the threshold score at 70%, the customer's 67% score would not meet that threshold and the customer would see a generic offer that could be made to any customer, male or female.

If the stakes are high, for example, in a law enforcement application where someone's life trajectory may change, the organization may set the threshold at 99%. If the stakes are not as high they may set the threshold at a much lower level.

That's something that enterprises should keep in mind. This technology is still new, so obviously it's not perfect, and it should be handled with care. Also, like many emerging technologies, it lacks many regulations to govern its use. So far. Those regulations will likely be coming in the years ahead.

Still, are there privacy issues with collecting customer images, particularly in the age of GDPR and other new data privacy laws? A booth representative at one of these demos at NRF told InformationWeek that the images of customers are not retained. However, aggregated data about the demographics of the customers who visit a particular display is retained and analyzed to help retailers gain insights into their customers.

Should enterprises be experimenting with AI facial recognition software? That probably depends on the application and the level of risk that is entailed. For physical store retailers looking to gain an edge against their digital competitors, these applications could open up a world of data and insights that have not before been available.

Other machine vision technology that looks for matches of images of people against a database of known images has been used to fight child trafficking in the case of Thorn. Likely matches are surfaced by the AI and the human-in-the-loop makes the final determination of whether a match has been found. The benefit of using AI in this type of application, whether it is identifying missing children or identifying a suspected terrorist at a crowded sporting event in real time, is that the algorithm can analyze and make a match in seconds. But in these kinds of high-risk applications, having a human in the loop to make the final call is probably an important safeguard against mistakes in this nascent technology.

That's something that enterprises should keep in mind. This technology is still new, so obviously it's not perfect, and it should be handled with care. Also, like many emerging technologies, it lacks many regulations to govern its use. So far. Those regulations will likely be coming in the years ahead.

References

1. “Practical Statistics for Data Scientists” ORELLY
2. https://www.cs.toronto.edu/~tingwuwang/semantic_segmentation.pdf