INTERVIEW WITH PROF. IR. DR. CHEE SENG CHAN

Prof. Chan is a Full Professor with the Faculty of Computer Science and Information Technology, Universiti Malaya, Malaysia. He is leading a research team that specializes in computer vision and machine learning where his team has published more than 100 papers in top peer-review conferences and journals. From 2020-2022, he was seconded to the Ministry of Science, Technology and Innovation (MOSTI) of Malaysia as the Undersecretary for Division of Data Strategic and Foresight, as well as the Lead of PICC Unit under COVID19 Immunisation Task Force (CITF). He was the recipient of Top Research Scientists Malaysia (TRSM) in 2022, Young Scientists Network Academy of Sciences Malaysia (YSN-ASM) in 2015 and Hitachi Research Fellowship in 2013. Besides that, he is also a senior member of IEEE, Professional Engineer (BEM) and Chartered Engineer (IET). Prof. Chan is also the founding Chair for IEEE Computational Intelligence Society, Malaysia chapter, and is currently an Associate Editor of Pattern Recognition (Elsevier).

What is the current focus of you and your team's research?

The current focus of my research team is more on the security, in particular we are very interested to look into how to protect the ownership of deep learning models. This is because as a researcher, we know that it is not easy to train a successful and commercially viable Deep Learning model. For instance, we spend a lot of time, money, and resources to do so, but at the moment, there is no ownership protection at all on this very valuable deep learning models. That is why recently we have been working with WeBank (a private online bank founded by multiple Chinese companies including Tencent Holdings Ltd.) on looking into the possibility to create a technology to protect the ownership of deep models.

Our approach to this problem is not application centric at the moment because we are targeting types of Deep Learning models in general. We started off with protecting the deep learning Convolutional Neural Network (CNN) and after that we move to Generative Adversarial Network (GAN). The main reason is that in common CNNs and GANs, the inputs and outputs are totally different. In CNNs, you usually input an image and get a classification result while for GANs you would input a latent noise and the output would be

an image. Some CNN and GAN models would eventually have images as input and output as well, but we mainly look at the common difference between their inputs and outputs for our work. We also further extended our work to RNN recently, with the same intuition whereby a common RNN input is a string of text and the output is also a string of text.

So the way we apply our techniques to CNN, we may not be able to apply to GAN in a simple manner due to the nature of the input, and seems that it cannot be applied to RNN as well. So that is why at the moment we are not looking at application centric but rather at the nature of the deep learning model itself. As of now, we have covered most of the basic architectures that is available in the literature including, models where the input is an image and the output a regression, models where the input is an image and the output is an image, the input is a noise latent vector and the output is an image, and lastly the input is a text the output is also a text. As a summary, we have covered most architectures that is popular in this domain.

From your experiences, how has the research landscape changed from when you first started till now?

I think with the emergence of Deep Learning we can see that there are exciting models that can be put into the commercial market compared to last time. This is because of the power of the deep learning algorithms and also the power of the digital data that is available now compared to last time. Now almost every device that we use is digital-based, no longer analog. Because of this, we are getting more and more data now. So [in terms of visual data] from the "classical" 2D image, now most people have gone to work on video, and also probably beyond 3D. These had been the changes [I've seen throughout the years].

With many research as well as industrial advancements claiming to incorporate or innovate with AI, what is your perspective on this trend?

Now the industry has been very excited due to the financial gain that they can get. I would say in overall, the industry nowadays is very excited about the emergence of Deep Learning but not a lot of industries eventually can sustain for a long time because of the lack of effort to build their own deep model. You need a lot of financial resources in terms of hiring the correct people and then have enough infrastructure to build a deep model. So at the moment, almost all the current start-up companies have no issues for the first two years of business because they can rely on open-source codes to have their customer base. However, once they move to year 3 and above, which I call the "sustainable time", they might have a hard time because of competition where they may be no different to their rivals [that continue using open-source solutions]. At this time, the company would have also grown and the financial requirement to sustain the company is higher now compared to when they just started. So the challenge for most of the companies eventually start in year 3. That is why recently, we also can see that a lot of technology companies have retrenchment because it is no longer viable to invest a lot of resources. We can see that the benefits or the return on investment (ROI) is quite marginally small from one to another. That is why companies now would need to look at how to really sustain in the current competitive market.

(Quite a lot start on trendy type of approach and go for open source because they thought that is what they are going to use)

Yes, that is why for those start-up companies, you can see that those very successful start-ups eventually do have their own algorithms. Those that are able to sustain beyond year 3 and above, we always see that they not just have their own technology, but they are also pursuing research in their area. An example of successful start-up is YOLO (You-Only-Look-Once deep learning object detection). YOLO is from a start-up company and

now we know there are up to YOLOv7 [for their object detector], so the researchers are still improving their "product" and they are still active in research including publishing research papers, so on and so forth.

I think publishing now is not like the conventional where it is only centric on academia, but companies now, in order to survive long enough, they need to start to look into some research element so that they can be differentiated even though very slightly from their rivals. This is so that they can be unique in their own domain to attract unique customers. We all know that deep learning solutions is not one-size-fits-all as it has always been customized to a certain application and if you have your own technology in a particular domain, then you will always be able to attract your type of customers that will eventually become your loyal customer in the future. So that is why, to have your own technology, and then move on to improve your technology is very important.

So the main message here is that you would definitely need to do (at least some) research. A lot of people always say that research papers are only for academia but it is no longer true because when you are able to publish your papers in very reputable conferences, from a company's perspective, it can give investors and clients more confidence in the company. This is because publications eventually tell the world that you may already have a new technology within the company, just that due to some kind of constrain such as hardware, the solution is not yet efficient or feasible financially to be deployed. The publication is one of the proof that the company already have a future solution waiting. I think this is very important but has been overlooked by a lot of start-up companies, particularly in Malaysia.

Nowadays, many tools and resources are open and accessible to anyone and everyone to devise their own AI projects and solutions, would this be a concern especially from the ethical side of things?

I think this is very important when it comes to ethics, and a lot of people have shown that it is possible to use technology [for ethics]. For example, in some of our work that we have shown, it is possible to use technology to protect deep models [a part of ownership ethics]. Some researchers in the domain of explainable AI have also shown that it is possible to use certain solution to make the model "more ethical" by knowing what is happening behind the scenes. But unfortunately, policy-wise is not ready. So that is the hiccup here because ethics are not merely just technological, you need lawmakers to come up with certain guidelines or policies.

At the moment, this is a work in progress because we know that it is not easy to come up with a policy that would be agreed by every parties and worse still the real understanding of any AI model is still in quite an infancy stage. In most cases, we still do not really know why an AI model behave in such a way. However, I do see efforts on improving ethics not only in terms of how we should use a model, but also on how should we use the data. For example, a particular set of data can be used to train a model for "good", but at the same time it can be used to train a model for "bad" purposes as well. How do we govern that? In my opinion, unfortunately, we are not there yet although there are some laws in Europe and also China for such protection in their early stages. However, these are mostly to tell that one would need consensus to use data, including the consent of the individual whose data is captured by even a CCTV, otherwise an alternative route away from the CCTV has to be provided by the developers.

In Europe, there is the General Data Protection Regulation (GDPR) that provides such protection to data. But what is still lacking is the governance of the AI's behavior. What if the AI acts

worse than expected, who would be the one responsible for the model's action? The company, the inventor, or eventually the user? At the moment we do not have a clear answer to this, so that is why there is still a long way to go when it comes to ethics.

(And because from the scientist perspective, understanding the AI also is still a work in progress so it is hard for the policy makers or even the public to even understand further.)

Exactly. As we all know, underlay of all these AI models are all algorithms achieved by some mathematics. But we also know that the real world environment keeps on changing from time-to-time and human behavior change as they age too. The data we use to train the model are typically historical data. There is no guarantee people that behave one way in the past will have the same behavior in the future. There are still a lot of such uncertainties in the real world environment where we try to apply algorithms on, so it may not be able to adapt well to this.

Most consumers would have used some form of AI technology and are focused on the convenience they provide, but do you think they are sufficiently aware of the potential negative implications that such tech would bring to their privacy?

I think everyone, even myself are very excited with all these technologies because no doubt that the advancement of technology has really improved our lives. It gives us more luxury to spend time with family and loved ones, and so on and so forth. But eventually none of us look into the [potential] negatives of it because we enjoy the benefits more than the so-called negative. However, we as an inventor or researcher in this area, we must be aware of every single possibility of negative impact that might happen so as to safe guard everyone.

We must know that, we have been enjoying the benefits of technology like AI because there are currently no rules and regulations. For example, the situation is just like driving on the highway. If there is no speed limit, users can drive as fast as possible and enjoy the shorter travel time from A to B. However, if an accident happens due to a lack of safety consideration, the consequences are very serious. Worse still is how to decide who to be held responsible in such a situation. From the consumer or user's point of view, they are only using the technology and service. A driver is only driving as fast as possible as there is no speed limit in place with the presumption that safety measures have been put in place by the service providers, such as road barriers, road quality, and then from the car manufacturers, a car that is well equipped with safety systems to handle collisions. This is the hypothetical situation that we have with AI right now.

We simply do not have any regulations around the word to dictate when A can or cannot be used. We also do not have limits on how far we can use the AI in a given population or conditions. That is why we can still enjoy a "free ride". The pro would be that the technology can improve a lot but the "side effect" would be, unbearable consequences if problems arise, especially from an ethical perspective. So I think what we need now is a check and balance.

There has been a saying from a movie, "Your scientists were so preoccupied with whether they could, they didn't stop to think if they should." Do you find that current day AI or computer scientists to have such a problem?

As a scientist and researcher, we would always be excited about technology, there is no doubt about that. But as I mentioned, it is because we have been enjoying the "free ride" [due to no regulations], we may eventually not think if we should do something or not because as a researcher, we go into it with a genuine attempt and a purpose. However, somehow, the work can be reversed and used against humans by someone else. So in such case, as I said, policies would be very important. There is no standardization so far and we have to be careful on what we choose to use or improve.

Based on your observations, has there been sufficient ethical awareness among computer scientists and the public?

I would say some of the researchers might be aware of this but definitely not the public. Probably 80% of the public is not aware because they are on the consumption side of things, enjoying the benefits and there is also not much information provided. There is a lack of awareness for example when they pass through an area with CCTV monitoring, and their data has been used as part of the training for an algorithm that no one had informed them about.

For some companies too where they are using face recognition systems and similar touchless mechanisms due to the pandemic, there has been no information revealed to consumers that their data has been captured by the devices and how long would it be kept. Matured industries like finance, the institutions have clear guidelines that details what would be the data used for, and how long it would remain with their servers, for instance 3 days, 5 days, and then it will be permanently deleted. There does not seem to be these kind of information related to AI.

Another simple example is social media. Often it does not seem that permission has been given to e-commerce platforms to trace our search history. But apparently, most of us has an experience where our search terms for a certain product in a search engine will somehow automatically appear as an advertisement in the social media platform as well as the e-commerce platform that we commonly use. To me, this is some kind of tracking that was done without my explicit permission [which is a breach of ethics]. Can I make a police report on this? It may not have any actions because based on current laws that I am aware of, there is nothing to be done. So as much as we want to use technology as much as possible, at the same time we also want to be protected. Unfortunately, the protection part is not there yet.

Has there been notable efforts to improve ethical accountability in computer science research?

I think there is a lot of efforts that is ongoing, such as the data protection act [of different countries]. We would start with data first, such as the European GDPR and a new California Privacy Rights Act (CPRA), and slowly move on from there. Unfortunately, policies are not something that can be done within a day. It usually takes years to be endorsed and passed by governments. I would say that it will be a long journey ahead because it seems to me, every country would have their own view on how data [and eventually AI] can and should be used.

Unity on this matter that can cut across the world will not happen in a short time or in the near future because we understand that there will always be disparity between developed, developing, and under-developed countries when it comes to technology. Also bear in mind that related policies will also need to involve cultural aspects as come matters are acceptable to certain countries and regions but not the others. So if we were to find a one-size-fits-all policy, it will be challenging. However, having some form of restrictions can be done soon. The community from academia and lead technologists are trying to help governments in various parts of the world to see to it. But as I said, it still needs time.

What should be the way forward since technology such as AI is ubiquitous to most consumers?

At the moment, technologies have shown and proved that they are very useful but now is the time for the policy makers to really sit down to come out with a check-and-balance. When this technology can be used and when it should be used? What are the terms and conditions to be set? If we do not do that soon, the more advance that we go, the harder it is for us to track all these changes. Especially nowadays where the world is on a full digital transformation. We really need to know now, and govern now or else it will be out of control very soon. So it is not about slowing down the technology but to catch up with the policy, that should be the way forward.

Any parting words for those who are following the development and trends of technology and AI?

For me I think, we definitely need technology to improve our lives. But having new technology is always an unpleasant thing for humans because humans always have a nature for reluctance of change. We can see through the industrial revolutions from 1st to 4th now. When a technology or a new invention has been put in place, always people have fear. For example, losing work opportunities and so on. If you look at the 2nd industrial revolution, from riding on a horse to the used of a car, people had reluctance on that. Up until now we have cars everywhere and then ride-hailing service like Uber, people also reluctant to that. In the coming future then might be worse with autonomous cars. So I think we need to look at the pros and cons on this. No doubt that when a technology an invention is been introduced, there will be a change of the job market but I would say that is how life is.

Regardless, all these technologies that have been put in place are always human-centric. It is the knowledge of humans that are represented by a set of algorithms, or mathematical equations. So a lot of technologies are always looking at humans. So I would say that as long as we humans are able to understand the works, and then having the policies to govern that, I think humans and technology can always work hand-in-hand to continue to improve human life. Just that unfortunately, at the moment we do not have a policy to govern AI so it creates some kind of fear in certain communities. Once this is resolve, I think everyone will know their position in the world, including technology. This is because now technology is everywhere, it is borderless without governance, yet humans are governed by certain policies which causes an imbalance. So we need to balance it so that humans would be able to enjoy more of this with less fear.