Artificial Intelligence and New Level of Fake News

S Nazar¹, M R Bustam²*
¹Departemen Sistem Informasi, Universitas Komputer Indonesia, Indonesia
²Departemen Sastra Inggris, Universitas Komputer Indonesia, Indonesia

Email: *muhammad.rayhan@email.unikom.ac.id

Abstract. The purpose of this study is to increase the awareness toward contents in the internet, like fake news or hoaxes. It focuses on internet contents made with artificial intelligence or AI. The method of this study used qualitative methods. The method is used to describe the people’s readiness toward fake news made with the help of artificial intelligence (AI). Besides, questionnaire is used to understand people awareness toward fake news. As the study focuses on one the AI technologies, Deepfake is taken for the research subject. The result shows that videos made with Deepfake are hard to tell if they were fake. Other than that, access to software implementing Deepfake is pretty easy to get; the example is faceswap, an open source project that is available and easy to use. Deepfake is useful in the film making industries, but recently it gets to the surfaces and is used to make fake news.

1. Introduction

In this globalization era, technology is used by people in any age, any professions, and even in any business. Information Technology (IT) helps companies to develop. IT is growing rapidly from year to year [1]. There is so many companies with technology base today, for example is a startup. Most of current business is running by using digital world as its own market. The digital world – and that includes its various industries – differs in multiple dimensions from the physical world and its industries, for instance in the areas of marginal costs in production, transport and storage, as well as the transport and production speeds [2]. This gives more profit to companies in any sizes, especially after internet becomes the link between physical and digital world.

Nowadays, peoples have smartphone and capable to access internet. People uses internet to get most of their information needs, whether is that news or rumors from their social media. Peoples choose internet as their main resources for information is because how easy it is to use and the speed. Other than that, it also gives the freedom for people to access many websites in one sit [3]. Not only that, it’s also easier to share information with the share button given in social media and news site. However, not all news in the internet is real. It’s one of the weaknesses of internet as a media compared to printed media like magazine or newspaper. Fake news concept isn’t a new thing; it’s already there before internet, but with different function compared to recent fake news. The old fake news is a parody or simply a fake news show. Their news stories were called “fake” not for their content, but for parodying network news, applying sarcasm and comedy to discuss real public issues [4]. Nowadays fake news is information that formed like real news but not in organizational process. There are some important components that characterize fake news, first is the information is inaccurate, second is having element of mimicry and third is the senders have the intentions to fools the readers [5]. There is many fake news in the internet. Therefore, the internet users start becoming more aware to fake news. A lot of news have some opposing information between one to another is one of the reason. Other than that, even if an individual does not clearly identify which news item is true and which is false, the presence of conflicting viewpoints indicates that at least one news item is
likely untrue [6]. Fake news currently handled pretty well with the appearances of fake news detection software with a good accuracy. This software made with AI and using algorithm like BLC [7]. All of those software capable of detecting text based fake news. However, recently fake news also appear with photos or videos that convincing enough for people to trust and with AI fake photo/videos also became easier to make. Deepfake is an AI tech that have function to swap faces from videos with other people faces can make the fake news industry to another level. Deepfake videos are appearing in social media and news, posing a significant technical challenge for detection and filtering of such content [8].

The purpose of this study is to increase the awareness toward contents in the internet, like fake news or hoaxes. This study used a qualitative method. This method is used to describe the readiness of the public for false news that is made with the help of artificial intelligence (AI). In addition, questionnaires are used to help people understand the awareness of false news.

2. Method
This study observes few other pieces of study about fake news, artificial intelligence and Deepfake. Qualitative method is used to discover the people’s readiness toward fake news made with help of artificial intelligence (AI). Besides using other pieces of study as a basis for the observation, we also learn one of Deepfake application that is available to public and can be used by anyone. Questionnaires are also given to college students to get to know what people think about this topic.

3. Results and Discussion
There is a lot of artificial intelligence (AI) being used today. As its name, artificial intelligence has the ability to learn. AI can learn by doing some simulations with genetic algorithm [9]. AI can also learn by giving it a lot of data or called as training data. The more data given for the AI to learn, the result will be better and more accurate. Besides the amount of data, the quality of the data sets also affects the result. This learning process will take a lot of time, but as computer goes there is always a way to optimize it by tweaking the used algorithm or formulas [10].

Like it has already mentioned before, AI trained by using data which mean the processing speed is up to the computer’s speed used to train it. This process is fast compared to the speed of a human. For example, AI can be trained to learn thousands of cases in a week, while human needs months or even years. Some AI that made to play a game like poker, it is proven they beat professional player [11]. This reality may be scary because human is beaten by machine in a case that’s not math.

AI make decision according to the data sets that given when training and not with programming. This make AI is one of the fastest software with one important thing, which is the data set to train the AI is available or atleast collectible. With a lot of AI in our world there might be some changes in the industry caused by some professions is better done by machine [12]. This also might affect jobs with creative requirements like an artist. This changes are actually happen recently caused by companies start using chatbot instead of real peoples as customer services. The chatbot technology is reach a point where it capable to understand the users and answer with a certain chatting styles [13]. Soon we will live side by side with AI and we need to be ready with the risk that come with it.

One of the risk of AI is the possibilities of AI used in the wrong way. The power of AI is proven capable to beat a human in short amount of time, which mean it will be dangerous to give access of AI open to public. Most applications that implements AI can only be accessed by some parties or certain tech products, but there’s also some AI applications that give access to people who like to pay. There’s also app that give access to public, most of AI in this category can be considered as harmless because its simple function. However, there is also Deepfake app that open to public and Deepfake is can be dangerous. This is because of Deepfake can be used to send hate speech or fake news on the internet. One of the open Deepfake applications is faceswap. Faceswap is open source application and everyone can use it (See Figure 1).
Figure 1. Faceswap Logo

Faceswap is Deepfake app that developed to run in Windows, MacOS, and Linux. According to its GitHub page, it has at least a thousand of peoples who use this application. The application is pretty simple and easy to use even for computer users in general. Knowing Deepfake can be misused; this is dangerous enough because of a lot of people can use this application. Deepfake nowadays being an issue and grab some people’s attention because of how real looking it is. If Deefaked videos get shared over and over on the internet, it will be a chaos because of the Deepfake’s result looks real enough to convince people to trust that it is real (See Figure 2).

Figure 2. Faceswap GitHub Page

Faceswap has simple interface that easy to use (Figure 3). The application has three main features which is extract, train, and converts.

- **Extract**: has function to detect faces from a video and extract it into series of images (Figure 4).
- **Train**: has function to train the app to understand and able to recreate the faces to be used as the source or the face to be the swap source.
- **Convert**: has function to create the result image or video with the replaced face what usually be called as Deefake video.

The work flow of Faceswap is extract, train and then converts. Every step take times especially if the computer used doesn’t have high specification. The longest process is the training, it can eat up to weeks depends on how many the images or how long the videos given is.
If explained simply, the first process in Faceswap is to detect the faces from source videos to be extracted into series of images in order (see Figure 4). The face detection on Faceswap is good enough even when the face is a little bit hidden. The results then will be used in the next step as the training data. The training menu needed the extracted series of face images from the original faces and also the extracted faces of the target faces. The training process will take a lot of time and will result a model file of the learned faces. The model file then will be used on the next step to produce the Deepfake video where the face is swapped.

As mentioned before, the video result from Deepfake is pretty convincing for internet users and hard to tell the differences from a real video. These videos now been spreading on the internet with
some reasons, there is some videos that only for entertaining purpose. However, there is also some that used to spread fake news. Few years back, people have been busy with a lot of fake news all over the social media. This is actually makes people to be more aware of fake news and also make people do some action to fight fake news. There are a lot of applications that capable to detect if the news is fake or real with the help of AI. However, now the case is different. Fake news now spread also in video format and not just text, so those applications cannot be used to fight this new type of fake news. Other than that, most people also consider a video as a proof of fact. Not a lot of people can do video editing that good enough to spread fake news, but with Deepfake it becomes a lot easier.

This study continues with giving questionnaire to some college students. All of them say Deepfake is really risky to be misused. Most of them also experienced getting fooled by fake news on their social media because of that they said video by Deepfake is can be used to trick a lot of people and makes chaos. However, most of them think that they can tell the differences from real and Deepfake videos by cross-checking the information by going to the internet or by watching more carefully. Moreover, there is also people who says the result of Deepfake is looks so real and not altered in any way. Some of the participants recommends to close the access to the software that uses Deepfake, but it’s not effective reminded with everything on the internet is never really gone. Some of the participants also recommend increasing the awareness of news on the internet even if it was assisted with images or videos. There is also some whose recommend to give socialization about Deepfake and share awareness about it, so then people know and aware about Deepfake videos.

Behind its capabilities to produces videos that hard to tell if it’s real, but there’s must be a differences between computer generated images and images captured by cameras. One of it is the appearance of artifacts on Deepfake video that can be used as the basis to tell if the videos are fake or not. One of the study that has been done [14], successfully detect Deepfake videos by doing analysis by the found artifacts. Same with fake news detection, Deepfake detection also made with the help of AI. However, Deepfake will always get better and then the Deepfake detection too must get better because if not Deepfake will be improved by using the detection data so it will be much harder. Besides, there are a lot of AI in development which is very possible to be misused by some peoples and that mean we need to be ready for the risk of AI.

We now are in a position where we use AI to fight another AI, which only increase the number of AI and not reducing it. In the questionnaire also includes questions about the need for law about the usage of AI, every participants agree if that kinda stuff is needed in this era. But, rules are often late to be made specially with technology related rules. In general, rules about tech usually be made after a case happen.

4. Conclusion
Artificial intelligence (AI) starts live on our side in daily life. AI can be used to help humans in a lot of things, simple or complex. However, no doubt if AI also comes with some risks that never been imagined before, like what happens with Deepfake. Deepfake became a real problem that needs public attention just because of the misused scenario with it. Deepfake itself really useful in film making, but just because of the misused cases it has bad reputation in the media. The face swapping features of Deepfake is no doubt make realistic looking video, but the world is not ready for it. Most people still does not know about Deepfake, so they might think Deepfake videos as a real video that is not altered or computer generated. We might be able to handle this AI problem with another AI, but how long it is going to be effective without making the AI situation worse. It might be back to us, how we aware about AI and how we are going to use it.

Acknowledgement
We are gratefully for the support from the Rector of Universitas Komputer Indonesia.

References
[1] Soegoto, E., & Luckyardi, S. 2019, May. Enhancing Student’s Competitive advantage in Technology Based University. In Proceeding Interuniversity Forum for Strengthening Academic Competency, 1(1), pp. 224-231
[2] Fleisch, E., Weinberger, M., & Wortmann, F. 2015. Business models and the internet of things. In Interoperability and Open-Source Solutions for the Internet of Things, pp. 6-10.
[3] Aldwairi, M., & Alwahedi, A. 2018. Detecting fake news in social media networks. Procedia Computer Science, 141, pp. 215-222.
[4] Paskin, D. 2018. Real or Fake News: Who Knows?. The Journal of Social Media in Society, 7(2), pp. 252-273.
[5] Nyilasy, G. 2019. Fake news: When the dark side of persuasion takes over. International Journal of Advertising, 38(2), pp. 336-342.
[6] Torres, R., Gerhart, N., & Negahban, A. 2018, Januar. Combating fake news: An investigation of information verification behaviors on social networking sites. In Proceedings of the 51st Hawaii International Conference on System Sciences.
[7] Conroy, N. J., Rubin, V. L., & Chen, Y. 2015. Automatic deception detection: Methods for finding fake news. Proceedings of the Association for Information Science and Technology, 52(1), pp. 1-4.
[8] Güera, D., & Delp, E. J. 2018, November. Deepfake video detection using recurrent neural networks. In 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pp. 1-6.
[9] Mauluddin, S., Ikbal, I., & Nursikuwagus, A. 2018. Optimasi Aplikasi Penjadwalan Kuliah Menggunakan Algoritma Genetik. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 2(3), pp. 792-799.
[10] Salimans, T., & Kingma, D. P. 2016. Weight normalization: A simple reparameterization to accelerate training of deep neural networks. In Advances in neural information processing systems, pp. 901-909.
[11] Brown, N., & Sandholm, T. 2018. Superhuman AI for heads-up no-limit poker: Libratus beats top professionals. Science, 359(6374), pp. 418-424.
[12] Zanzotto, F. M. 2019. Human-in-the-loop Artificial Intelligence. Journal of Artificial Intelligence Research, 64, pp. 243-252.
[13] Xu, A., Liu, Z., Guo, Y., Sinha, V., & Akkiraju, R. 2017, May. A new chatbot for customer service on social media. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, pp. 3506-3510.
[14] Matern, F., Riess, C., & Stamminger, M. 2019, January. Exploiting visual artifacts to expose deepfakes and face manipulations. In 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW), pp. 83-92.