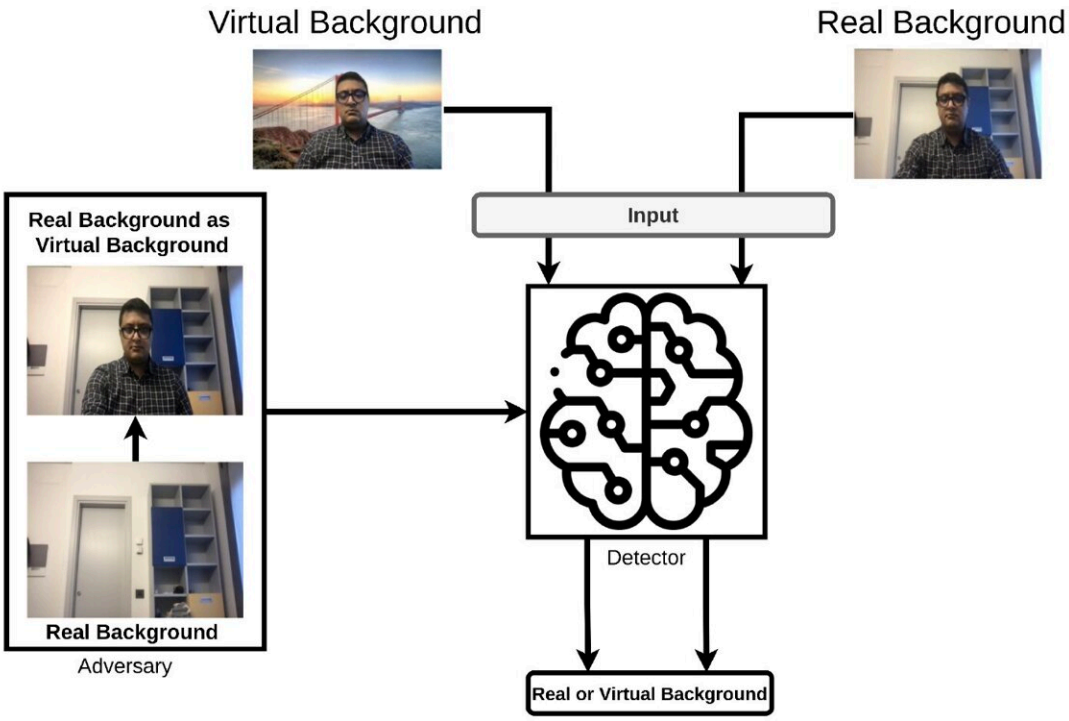
A strategy to discern between real and virtual video conferencing backgrounds

May 17 2022, by Ingrid Fadelli



Credit: Nowroozi et al.

Video-conferencing platforms such as Skype, Microsoft Teams, Zoom and Google Meet allow people to communicate remotely with others in

different parts of the world. The COVID-19 pandemic and the social distancing measures that followed led to a further rise in the use of these platforms, as it increased remote working and virtual collaborations.

Most video-conferencing platforms now also allow users to use virtual backgrounds, so that they don't need to show their home environments to their co-workers and to reduce the risk of distractions. These virtual background can be i) real (current), ii) virtual (e.g., a seaside landscape or outer space), and iii) fake, which is a real but not current background. While being able to change the background increases users' privacy, fake backgrounds can also be used with malicious intent, to give the impression of a false location, for instance suggesting that a user is at the office when he is actually at home.

Researchers at Sabanci University in Turkey, Florida International University in the United States, and University of Padua in Italy have recently developed a tool that could be used to distinguish between real and virtual backgrounds in video-conferencing platforms. Their method, introduced in a paper pre-published on arXiv, was found to successfully discern between real and "artificial backgrounds" in two distinct and common attack scenarios.

"Recently, scholars proved that most machine and deep learning techniques are vulnerable to adversarial attacks in multimedia forensics," Ehsan Nowroozi, Berrin Yanikoglu, Yassine Mekdad, Selcuk Uluagac, Simone Milani and Mauro Conti, the researchers who carried out the study, told TechXplore via email." In fact, with the pandemic conditions, several meetings have been carried out remotely through video conferencing software that enables participants to use a virtual background for privacy concerns."

Some past studies demonstrated the possibility of adversaries revealing the real environment of a participant by leaking pixels from the virtual

background. However, companies may also have a legitimate need to know if the user is indeed in the presented background.

The key objective of the recent work by Nowroozi and his colleagues was to build a system that can robustly distinguish between real background versus a virtual or fake one in a video-conferencing call. The method uses deep learning techniques to distinguish between real vs fake or virtual backgrounds with high levels of accuracy. In addition, their detector can be used to detect adversarial attacks and fake backgrounds across a wide range of video-conferencing platforms.

"The system works by considering the six co-occurrence matrices between the three color channels of the background," the researchers explained. "In a fake or virtual background, due to the static nature of the background image, we don't see the changes in the spectral domain", says Nowroozi, "but finding the relationship between channels is challenging. Therefore, the only way is to use cross-band co-occurrences across the channels and feed them to the deep-learning based detector."

"We are the first group that provides a CNN-based model capable of distinguishing between real background versus a virtual or fake one in a videoconferencing call," Nowroozi and his colleagues said. "Moreover, we achieved a high accuracy of 99.80% in the case where the detector is aware of the attack and high robustness even in the case of an unaware detector."

In the future, the CNN-based detector developed by this team of researchers could be used to confirm the authenticity of video-conferencing backgrounds in professional settings, as well as in law enforcement and judicial settings. In the meantime, Nowroozi and the rest of the team plan to continue working on their detector to improve its performance and generalizability further. Ideally, they want this detector to be applicable to the most popular video-conferencing platforms,

including Zoom, Google Meet and Microsoft Teams.

"Our future research will first consider the case of whether an adversary can deceive the detector if it can access the cross-band co-occurrences," Nowroozi and his colleagues added. "Secondly, we plan to evaluate our detector in the scenario where the attacker considers a moving virtual background (e.g., clips)."

More information: Ehsan Nowroozi et al, Real or virtual: a video conferencing background manipulation-detection system. arXiv:2204.11853v1 [cs.CV]. arxiv.org/abs/2204.11853

Machine learning techniques for image forensics in adversarial setting. Ph.D. Thesis (2020). theses.eurasip.org/theses/859/ … for-image-forensics/

Ehsan Nowroozi et al, A survey of machine learning techniques in adversarial image forensics. arXiv:2010.09680v1 [cs.CR], arxiv.org/abs/2010.09680

Shijing He, Yaxiong Lei, The privacy protection effectiveness of the video conference platforms' virtual background and the privacy concerns from the end-users. arXiv:2110.12493v1 [cs.HC], arxiv.org/abs/2110.12493

Jan Malte Hilgefort et al, Spying through Virtual Backgrounds of Video Calls, *Proceedings of the 14th ACM Workshop on Artificial Intelligence and Security* (2021). DOI: 10.1145/3474369.3486870

Christopher Wampler et al, Information Leakage in Encrypted IP Video Traffic, *2015 IEEE Global Communications Conference (GLOBECOM)* (2016). DOI: 10.1109/GLOCOM.2015.7417767 , https://ieeexplore.ieee.org/abstract/document/7417767

Mauro Barni et al, CNN Detection of GAN-Generated Face Images based on Cross-Band Co-occurrences Analysis, *2020 IEEE International Workshop on Information Forensics and Security (WIFS)* (2021). DOI: 10.1109/WIFS49906.2020.9360905