Deepfake

A deepfake is originally defined as a video of a person in which their face or body has been digitally altered so that they appear to be someone else, usually used to spread false information.
It is the 21st century's answer to Photoshopping. The term "deepfake" came from its origin as we use a form of artificial intelligence called "deep learning" to make images of "fake events". Deepfakes are basically synthetic media created using artificial intelligence (AI) techniques. They're mainly used for either entertainment purposes (pornography included) or political ones.

How are they made?
The process of creating a face-swap video involves a few steps. First, a vast number of face images of the two individuals are processed using an AI algorithm called an encoder. This encoder then identifies and learns the common features shared by the two faces, while also compressing the images on the side. Subsequently, a decoder AI algorithm is trained to reconstruct the faces from the compressed images. Since the faces involved are bound to be different, we see that separate decoders are trained to reconstruct each person's face. To finally execute the face swap, encoded images are then simply fed into the "wrong" decoder.

Another way to make deepfakes uses what's called a generative adversarial network, or Gan. A Gan pits two artificial intelligence algorithms against each other. There is a Generator and a Discriminator. The Generator generates fake samples of data(be it an image, audio, etc.) and tries to fool the Discriminator. The Discriminator, on the other hand, tries to distinguish between the real and fake samples. The Generator and the Discriminator are both Neutral Networks and they both run in competition with each other in the training phase. The steps are repeated several times and in this, the Generator and Discriminator get better and better in their respective jobs after each repetition.

Despite the fact that Deepfakes pose significant threats to privacy, as they can be used to create fabricated content without the consent of the individuals involved, they still could be a source of knowledge as well as entertainment. It could be used for educational purposes, historical reconstructions, and even enhancing visual effects in the entertainment industry.
If you are wondering about how to tell the difference between an original and a deepfake, it is to be noted that detecting deepfakes requires advanced analysis techniques that often involve AI algorithms. Researchers are continuously developing methods to identify inconsistencies, artifacts, or abnormalities in videos that indicate manipulation.

With the increasing ease of generating deepfakes, protecting personal privacy becomes paramount. Safeguarding personal information and educating individuals about the risks of deepfakes are crucial parts of the process. The rise of deepfakes present, in front of us, a complex and evolving challenge in the digital age. While deepfakes offer opportunities for entertainment and innovation, they also carry substantial risks for society, politics, and individuals. Proactive measures, such as technological advancements and legal frameworks, must be implemented to ensure the responsible and ethical use of synthetic media, and for the sake of safety and privacy too.

Reference1
Reference2