“All Around Me Are Synthetic Faces”: The Mad World of AI-Generated Media

Lucas Whittaker
Queensland University of Technology

Jan Kietzmann
University of Victoria

Tim C. Kietzmann
Radboud University & Cambridge University

Amir Dabirian
KTH Royal Institute of Technology & California State University

Abstract—Advances in artificial intelligence and deep neural networks have led to a rise in synthetic media, i.e., automatically and artificially generated or manipulated photo, audio, and video content. Synthetic media today is highly believable and “true to life”; so much so that we will no longer be able to trust what we see or hear is unadulterated and genuine. Among the different forms of synthetic media, the most concerning forms are deepfakes and general adversarial networks (GANs). For IT professionals, it is important to understand what these new phenomena are. In this article, we explain what deepfakes and GANs are, how they work and discuss the threats and opportunities resulting from these forms of synthetic media.

ANTICIPATING A “MAD WORLD”

Barack Obama’s public service announcement starts with the usual backdrop of American flags within the Oval Office. His distinctive vocal pauses and hand gestures lend credibility to his address about the modern threat of digital technologies and artificial intelligence (AI). But suddenly, his own address starts to take a strange turn, culminating in an alarming and out-of-character statement: “President Trump is a total and complete dipsh%t.” Wait, what? Obama pauses to clarify, “See, now I would never say these things, at least not in a public address. But someone else would.”
This video then introduces comedian Jordan Peele, who imitates Barack Obama’s voice. Peele’s facial expression and mouth movements morphed into Obama’s using FakeApp, a free tool. In the video, Peele leverages the credibility of the 44th U.S. President’s face and voice to warn the viewer that “how we move forward in the age of information is going to be the difference between whether we survive or whether we become some kind of [expletive] dystopia.”  

Published by Buzzfeed, the video reveals how so-called “deepfakes” can be created to impersonate public figures by others, including those with a potentially harmful agenda. But these deepfakes are not the only highly precarious media that test what we should believe to be true. Contrary to deepfakes and their ability to generate images that combine features of a source and target image (e.g., Peele’s and Obama’s faces), generative adversarial networks, or GANs for short, can create entirely new and lifelike, naturalistic content (e.g., faces of people who do not exist).

The recent increase of convincing, highly believable, and “true to life” deepfakes and GAN-generated media prepares us for a mad world in which we will no longer be able to trust that what we see or hear is unadulterated and genuine—a world in which “synthetic media” will force us to re-evaluate our very perception of reality.

SYNTHETIC MEDIA

The examples above illustrate a world where we not only live with the common digital content that surrounds us, for instance advertisements enhanced with apps like Photoshop or movies with computer-generated imagery (CGI) like special effects, but also with synthetic media. With the term “synthetic media,” we refer to all automatically and artificially generated or manipulated media.

It is important to keep in mind that synthetic media is an umbrella terms for a host of other media. Types of synthetic media, for instance, include synthesized audio (e.g., Google Duplex), virtual reality, and even advanced digital-image creation (beyond CGI, where expert systems are increasingly capable of automatically producing realism on a vast scale). The two branches that cause the biggest concern currently though, are deepfakes and GANs.

WHAT ARE DEEPFAKES AND HOW DO THEY WORK?

The deepfake phenomenon initially gained public awareness in late 2017 within online hobbyist communities. A Reddit user with the username “deepfakes” used AI algorithms to insert the faces of famous actresses into adult videos. After the computer code necessary to generate deepfakes became publicly available, online communities began to create more and more deepfakes, including the abovementioned Peele/Obama video. Before December of 2017, the term “deepfake” did not even register on Google Trends (a website that analyzes the popularity of top search queries in Google Search), but ever since it has been on a steady incline. Not even two years after the first appearance, in the fall of 2019, CNN reported that there were almost 15,000 deepfakes, nearly all of them were non-consensual instances of deepfake porn. However, there are many other applications of the technology used to create deepfakes, at this point mainly (but not exclusively) for entertainment purposes.

At first, these meme-like videos created by hobbyists were usually crudely constructed with obvious AI manipulation—but still demonstrated the immense potential of deepfake technology. For instance, a curious obsession with planting Nicolas Cage in popular movies arose, with viral videos depicting Nicolas Cage in roles such as Indiana Jones in Raiders of the Lost Ark and Lois Lane in Batman versus Superman. The past two years have seen deepfakes move beyond online communities and become created with increasing sophistication across an array of formats.

- Photo deepfakes can be created by swapping out faces and bodies within images.
- Audio deepfakes can create, alter and imitate voices, from audio sources or from text.
- Video content can be (deep)faked, with a moving face being able to be swapped or morphed.
with another, or the bodily movement of a person being replaced by someone else’s.

- To create the most perhaps sophisticated deepfakes, the above approaches can be combined to manipulate mouth movements and facial expressions alongside audio materials to have someone convincingly say things which they have never said.

At their core, deepfakes are the product of AI and the machine learning technique of “deep learning,” which is used to train deep neural networks (DNNs). On a very abstract level, DNNs resemble some computational principles also found in the brain. Their synthetic neurons, better known as “units,” perform simple nonlinear operations. Yet, when setup as a network of thousands and millions of units, these simple functions combine to perform complex feats, such as object recognition, language translation, or robot navigation. Importantly, the function of a whole network of units is determined by the pattern of its unit connections. To drive a network to perform the desired function, the connection strengths between units are adjusted via training on large sets of example data. In the case of deepfakes, such DNNs are trained as a central part of AI systems that automatically merge, combine, replace, and superimpose images and video over a targeted video to create a hyperrealistic, yet *fake* alternative content.³

Due to the requirement for large sets of training data that enable DNNs to adjust the millions of unit connections, individuals in the public eye, such as celebrities, actors, and politicians are particularly susceptible to becoming targeted by deepfakes as vast amounts of audio and visual content of them are widely available online.

To date, most available deepfakes are created by using a specific network architecture, known as an “autoencoder,” which specializes in generating real-looking, yet fake, facial images of a target person (please see the work done by Kietzmann *et al.*³ for an in-depth explanation of the underlying technology). It is important to keep in mind that autoencoders not only work with faces, though, and can be trained on a variety of different content (e.g., voices of people). To use autoencoders for deepfakes, they are fed with large numbers of facial images of a given person. Their task is to recreate the same image that they are presented with. While seemingly simple, the task is complicated by the design of the network architecture, which requires the image information to pass through an information bottleneck that applies significant compression. To solve this complex task, autoencoders learn to first extract more abstract facial characteristics and emotional expression from the input image (known as the “encoder” part of the autoencoder), and from there generate the output image (known as the “decoder”) that matches the input. As the geometry of faces is quite stereotypical, they lend themselves particularly well for such compression. As a result, the decoder part of the autoencoder can generate any image of the person it was trained on, whether such image previously existed or not.

To create deepfakes with autoencoders, two separate networks are trained, one for each person. To stick with our introductory example of Obama and Peele, deepfake artists would train two autoencoders based on image sets of either person. The trick that enables a transition from the image of one person, say Peele, to another, say Obama, is that the two networks are linked such that the connection strengths of the encoder part of both networks are kept identical. This implies that the network learns to not specialize on one person, but learns to recognize more general facial features that are common across the two people.

But how does this setup help to create deepfakes? The linked encoder parts of the autoencoder allow users to input an image of Peele into the encoder, and subsequently generates a matching image of Obama as the output. Importantly, this newly generated image of Obama will have the same facial and emotional expression as the Peele input image. This renders it particularly easy to take the newly created image and copy it into the input image, thereby swapping the two people.

As per Figure 1 (adapted from the work by Kietzmann *et al.*³), to create a deepfake image of a target person (Obama), step one consists of extracting the face from an image showing an actor that performs the wanted expression. As step two, the autoencoder then translates this source image into a novel image of the target person.
that directly matches the input actor in facial and emotional expression and head orientation. Importantly, the resulting generated image will not just copy over the pixels, say the smiling lips, of the actor, but generate a smile that is unique to the target person (e.g., the exact way Obama would smile). Step three consists of taking the generated image and copying it back into the original image. Instead of the actor, now the target person is shown in the same pose and expression.

**WHAT ARE GENERATIVE ADVERSARIAL NETWORKS AND HOW DO THEY WORK?**

While DNN architectures for deepfakes specialize in exchanging one person for another, DNNs can also be used to generate entirely novel content. This is the case for GANs, which, like autoencoders, originate from the family of “generative models” (as opposed to “discriminative” networks that can take images as input but are tasked to describe or classify what is being shown). Generative models can be used to create novel data that resembles the data the networks were trained on. As general as this statement may seem, the possibilities for creating content from GANs are endless. GANs were introduced in 2014, and while the first results, generating faces and written digits, were low in resolution, they clearly demonstrated the powerful capabilities of this new style of training networks. Today, GANs are used to generate high-resolution facial images of nonexistent people, to create pictures of imaginary breeds of dogs, to assist artists in their paintings, for example, by filling in colored details into line drawings, and can take existing images of low quality and generate high-resolution versions of them by “fantasizing” details that were not present in the original. By design of the underlying network architectures, the speciality of GANs is to generate entirely novel content that is strikingly similar to original, real images of people and things (see Figure 2 for examples of GAN-generated content). This renders them equally powerful and dangerous.

The key to understanding DNNs that enable the creation of deepfakes is that they in fact consist of two interlinked networks, each of which is trained to become an expert at generating one of the two people to be swapped later on. GANs, too, consist of two deep networks. However, instead of working together, they perform opposing roles. One network, the “generator,” is used to generate fake content from random input, say, images showing human faces. A second network, known as the “discriminator,” is fed with both fake and real content, and it is trained to be successful at determining whether a given input is fake. Akin to an arms race between money counterfeiters and the police, the generator improves if its generated fake image was detected as such. If instead the discriminator was fooled into mistaking a fake image as real, it learns from this mistake to prevent future error. The interplay of these two networks, both of which want to outplay the respective other, leads to incremental improvements on both sides. Once the networks
are trained, the discriminator is commonly discarded, and the generator is used to generate new content originating from previously unused random noise as input.

THREATS AND OPPORTUNITIES OF SYNTHETIC MEDIA

It is abundantly clear to the reader of this article that the technologies that enable synthetic media are very powerful. Synthetic media, and especially deepfakes and GANs, provide numerous threats and opportunities that we ought to be aware of—as we will need to question whether what we see and hear is authentic and unadulterated by others. Below is a nonexhaustive list of some threats and opportunities of synthetic media—a list that will certainly change and grow as deepfakes and GANs find wider application.

Threats

Unsurprisingly, the ability for users to create artificial realities using deepfakes and GANs is fraught with malicious potential. In particular, the believability and accessibility of deepfakes play significant roles within the growing threat that the technology represents. Deepfakes are being increasingly difficult to distinguish from authentic video, and the barriers to creation have lowered significantly with widely available mobile apps such as FakeApp and Zao enabling unskilled individuals to create their own deepfakes. Disconcertingly, the growing simplicity involved in creating convincing deepfakes, combined with our increasingly digitally documented
lives, will heighten the potential for them to be used for malicious purposes such as blackmail, intimidation, sabotage, harassment, defamation, revenge porn, identify theft, and bullying.\textsuperscript{3, 7}

The generation of nonconsensual videos is a disturbing application of deepfakes and GANs. It all started with actresses such as Natalie Portman and Gal Gadot in addition to other female public figures such as Michelle Obama, Ivanka Trump, and Kate Middleton who became victims of nonconsensual deepfake insertion into adult film scenes. To date, women remain the main victims of deepfakes. Content distributors such as Reddit, Pornhub, and Gyfcat have banned artificially generated pornography from their platforms, however, sexually explicit and degrading deepfake content can still circumvent these mainstream platforms and be widely distributed. This occurred in the case of Rana Ayyub, a self-described antiestablishment investigative journalist in India, who was the victim of a viral pornographic deepfake maliciously designed to humiliate her in the public eye which was widely circulated via Indian WhatsApp groups.\textsuperscript{8} Even those outside the public spotlight can be targeted, such as the case of an 18-year-old woman who reverse image-searched her photo out of curiosity only to find hundreds of images of her face inserted into pornographic scenes. After trying to remove the images and becoming an advocate against image-based sexual abuse, she became the victim of a deepfake pornographic video which was uploaded to numerous websites.\textsuperscript{9} Deepfakes are the next sinister breed of revenge porn which can make everyone potential targets even if they have never taken explicit photographs or videos of themselves (!).

Deepfakes and GANs represent the next generation of fake news and threaten to further erode trust in online information. Artificially generated video poses a greater threat of disinformation compared to text or image-based fake news due to how difficult the digital alteration can be to spot. People are inclined to believe what they see, and when combined with factors such as confirmation biases and social media echo chambers which facilitate the propagation of fake news, artificially generated content will further fuel the fake news crisis with their ability to undermine truth and confuse viewers. As malicious deepfakes become more commonplace, the public may even begin to lose trust within news and factual information.\textsuperscript{7}

Disturbingly still, deepfakes can further erode democracy and truth by creating a “liar’s dividend,” acting as a plausible scapegoat to genuine recordings of misbehavior and corruption. One particularly concerning scenario is the dismissal of authentic video evidence documenting human rights abuses, arguing that the content has been faked. Without proper detection technology, every video, even those that are 100% accurate recordings of real events, can be passed up as fake—everyone will have plausible deniability for any event caught on video.

The political sphere is particularly vulnerable to deepfakes and GANs intentionally created to deceive. The United States Senate recently passed legislation to better understand how foreign governments and domestic groups use deepfakes to damage national security and threaten American democracy. The ability for GANs to generate the faces of people who do not exist can result in political astroturfing. Facebook recently removed more than 900 fake accounts using GAN-created profile photos which circulated pro-Trump messages via social media.\textsuperscript{10}

Deepfakes will be yet another tool within state-sponsored disinformation campaigns to interfere with elections and create civil unrest. United States lawmakers have expressed concern that deepfakes will soon be used by malicious foreign actors, with Senator Marco Rubio stating that deepfakes would be used in “the next wave of attacks against America and Western democracies.”\textsuperscript{11} These deepfakes targeting politicians could be legitimized using similar tactics to those allegedly employed by Russia in their interference within the 2016 U.S. Presidential Election by their use of troll-farms to circulate disinformation. Alarmingly, deepfakes and GANs could be used by rogue agents such as terrorist groups. Using minimal resources, artificial realities could potentially be created of (for example) United States soldiers discussing or engaging in war-crimes while stationed in the Middle East, to serve the agendas of rogue agents attempting to radicalize and recruit individuals to join their cause.\textsuperscript{7}
Set in the context of the private sector, synthesized voice, created via deepfake technology, can be used for fraudulent activity. Using AI-based software to mimic the voice of a CEO, fraudsters were able to successfully request the transfer of $US243,000 into a fraudulent account during a phone call with the firm’s CFO, who was tricked to recognize the slight German accent and vocal melody of his boss during the fraudulent phone conversation.

Deepfakes also represent a major threat to organizations and brands, adding further weight to fake news stories already being fabricated to target specific companies. Fake news can cause significant economic impact, such as the fake news article which intentionally misquoted Pepsi’s CEO Indra Nooyi as saying that supporters of Donald Trump should “take their business elsewhere,” resulting in calls for boycotts and a 3.75% decrease in Pepsi’s share price. The weight of realism that deepfakes can contribute toward malicious agendas means that there is a need to plan for reputational damage sustained from, for example, a senior executive or figurehead being targeted by deepfake to say compromising statements.

Opportunities

Despite the insidious potential of deepfakes and GANs, they have exciting potential to do good. For instance, deepfakes can aid in the removal of language barriers which can constrain cross-cultural video content distribution, which might typically require supplementation with subtitles. Social intervention campaigns such as the Malaria Must Die campaign demonstrates how deepfakes can transcend language, with former English footballer David Beckham seemingly speaking nine different languages in a voice petition to end malaria.

Deepfakes are also being used to transcend language barriers within political spheres. Manoj Tiwari, President of India’s ruling Bharatiya Janata Party, recently embraced deepfake technology to directly speak to Hindi-speaking constituents. Originally a recording in English that criticized his political opponent, his video was consensually translated via deepfake into Haryanvi, a Hindi dialect widely spoken by his target voters. The deepfake had reportedly reached approximately 15 million people in 5800 WhatsApp groups.

Deepfake technology is also giving a voice to those who have lost theirs due to medical conditions such as motor neuron diseases. Using similar deep learning principles employed to create video deepfakes, Project Revoice (www.projectrevoice.org) uses generative AI from voice samples provided by vocally-paralyzed clients to create personalized synthetic voices.

The film industry can also greatly benefit from the implementation of deepfake technology, which can be used to de-age actors to a comparative level of costly CGI effects. Netflix’s The Irishman used CGI to de-age actors such as Robert De Niro, Al Pacino, and Joe Pesci to appear decades younger than their current selves, which reportedly drove the budget of the film to as high as $US175 million. Using free software called DeepFaceLab and only seven days, one YouTuber recreated Netflix’s de-aging effects and released a video comparing the CGI of the actors within scenes from The Irishman to the deepfake version of the actors. The deepfake recreation of the scenes was highly convincing and has even been hailed as superior to the costly CGI effects, which were reported as being “distractingly bad” and like “some hellish uncanny valley.”

Digital revival is an already established, yet a controversial practice within the world of cinema. CGI revivals include resurrecting Peter Cushing as Grand Moff Tarkin in Rogue One: A Star Wars Story and Paul Walker as Brian O’Conner in Furious 7. Though an ethical and potentially legal minefield, deepfakes can give filmmakers a cost-effective alternative to CGI resurrection by utilizing the vast audio and visual material of deceased actors. The Golden Age of Hollywood may yet rise again.

The potential for deepfake resurrection has already been realized beyond film. Tourist attractions such as The Dalí Museum in St. Petersburg, Florida have adopted deepfake technology to breathe life into the Spanish surrealist who passed away in 1989. After pressing a button next to a life-sized screen, Dali leaves his easel and approaches the visitor, talking to them about his artwork and the museum. Upon leaving the museum, Dali appears to the visitor once more to ask whether they would like a selfie with...
him, where he takes a photo of himself with the visitor which is delivered via SMS. When employed respectfully, such application of deepfake technology has incredible power to establish deeper connections with the deceased to create emotional experiences and provide richer insights into their lives.

Deepfakes offer boundless potential for personalized media creation. The highly popular Chinese app Zao enables users to swap their face over the actor within scenes from popular movies and TV shows, allowing anyone to be a star and share their creation with the world. This deep level of personalization combined with the increasingly accessible nature of deepfakes offers organizations new ways of engaging with customers. For example, a brand could release an app allowing customers to deepfake themselves into purpose-built advertisements or scenarios to share with their social networks.

Companies such as Artificial Talent (https://artificialtalent.co/) specialize in the creation of AI promotion models using GANs, with business clients able to customize the physical characteristics of the fashion models and the clothes they wear to create promotional campaigns without the need to cast human models. GANs can also be used to generate images of humans conditioned to form a specified pose. Brands are now able to generate models which are perfectly cast to reflect their brand image or promotional campaign without the need for a human model, circumventing scheduling issues, costly photoshoots, controversies the model may find themselves within, and even aging.

Deepfakes and synthetic AI models generated by GANs could be merged for the ultimate personalization of online customer experiences, such as online clothes shopping. Customers could provide basic physical characteristics to an online fashion store which generates their own personalized avatar to use for online fashion shopping. Further personalization could even occur with the customer being able to deepfake themselves as the model for a true visualization only rivalled by the in-store dressing room.

GANs can be used to stylistically transfer imagery. By being trained on landscape photographs and mimic collections of art styles (e.g., the entire works of Monet and Van Gogh) GANs can generate the original photographs in the style of Monet and Van Gogh, offering new ways to replicate artistic styles and generate new artwork. Anyone can become a GAN artist using Artbreeder (https://www.artbreeder.com/), which allows users to create and merge images to generate completely new artistic pieces constructed by GANs.

GANs can also be used to create superresolution imagery from low resolution inputs. Though the creation of high-resolution imagery from lower resolution input is not new, the technology can still struggle to remove noise and compression artifacts. GANs can optimize this process by creating a higher quality image than one that ever existed—“fantasizing” details onto the low resolution image. GANs could therefore be used to augment current applications of superresolution technology, which is used in contexts such as satellite and aerial imaging, medical image processing, facial image detection, text image improvement, and compressed image and video enhancement.

There are a multitude of further GAN applications which we cannot fully explore within the scope of this article, however, others include image creation using only text input, context-based pixel prediction to repair images with entire sections removed, detecting online spam reviews, and even music composition.

CONCLUSION

The “good old days” of purely analog and digital content creation and modification of media are numbered. Synthetic media are making fast inroads, and as technologies around deepfakes and GANs keep improving, we will see more and more applications that will challenge our current understanding of what is real and what is not, and that will put our sense of truth and trust to a test.

The task for IT professionals is to improve the technology of creating synthetic content while at the same time ensuring that “fakes” will be identifiable as such, the duty for lawmakers is to update our laws about creating, distributing, and sharing synthetic videos, images, or audio. The big challenge for us as everyday consumers...
is to stop believing everything we see and hear on social media, and instead to start thinking critically again and to question the “evidence” in front of us. All of this will take time, and until we all arrive at a common understanding of how synthetic media fit into our lives, it will be a mad world!

■ REFERENCES


Lucas Whittaker is currently working toward the Ph.D. degree with the School of Advertising, Marketing and Public Relations and Research Student with the Centre for Behavioral Economics, Society, and Technology, Queensland University of Technology, Brisbane City, QLD, Australia. His research explores how visual deepfakes can potentially be weaponized to target brands and investigates the role behavioral biases play within the acceptance of visual deepfakes. Contact him at ll.whittaker@qut.edu.au.

Tim C. Kietzmann is currently an Assistant Professor with the AI Department, Donders Institute for Brain, Cognition and Behavior (Radboud University), Nijmegen, Netherlands. In addition, he is a Research Associate with the MRC Cognition and Brain Science Unit (University of Cambridge). In his interdiscipli- nary work, he combines neuroscience with AI technologies to help better understand principles of neural information processing in the brain. Contact him at t.kietzmann@donders.ru.nl.

Jan Kietzmann is currently an Associate Professor with the Management Information Systems, University of Victoria, Victoria, BC, Canada. He is also an Associate Editor with Business Horizons. His research focuses on organizational and social perspectives related to emerging technologies. He received the Ph.D. degree in Innovation and Information Systems from LSE. Contact him at jkietzma@uvic.ca.

Amir Dabirian is currently the Vice President for the Division of Information Technology and as a Faculty Member with the Department of Marketing, California State University, Fullerton, CA, USA. He is currently working toward the Ph.D. degree with the Department of Industrial Economics and Management, KTH Royal Institute of Technology, Stockholm, Sweden, with research interest in employer branding. Contact him at amir@fullerton.edu.