Juan-José Boté-Vericad
Universitat de Barcelona
juanjo.botev@ub.edu

Mari Vállez
Universitat de Barcelona
marivallez@ub.edu

Image and video manipulation: The generation of *deepfakes*

https://doi.org/10.3145/indocs.2022.8

Boté-Vericad, Juan-José; Vállez, Mari (2022). Image and video manipulation: The generation of *deepfakes*. In: Freixa, Pere; Codina, Lluís; Pérez-Montoro, Mario; Guallar, Javier (ed.). *Visualisations and narratives in digital media. Methods and current trends*, (pp. 116-127). Barcelona: DigiDoc-EPI. https://doi.org/10.3145/indocs.2022.8

Abstract

The growth of fake news is nowadays a growing reality, leading to users feeling insecure when consuming information. Text-based news is perhaps the most manipulated, but the video is rapidly gaining ground. Technology allows content to be easily adulterated, leading users to become misinformed. In this study, we explain the different image, video, and audio manipulation techniques that are carried out with software and advanced audiovisual techniques. The most prominent methods are morphing and warping, together with machine learning techniques. Also, artificial intelligence is a critical element in the growth of fake video generation. This brings with it the need to identify the fake videos to verify the facts being told. It is also essential to understand social tolerance, especially in humour programmes, as some media outlets use these mechanisms. Moreover, it is analysed the importance of privacy policies that affect how the users' personal information is collected and their implications in their fundamental rights. Finally, it is concluded with the need for media and digital literacy campaigns in the education system to minimise this problem.

Keywords

Deepfake, disinformation, video manipulation, apps, mobile applications.

Título

La manipulación de vídeos e imágenes y la generación de *deepfakes*

Resumen

El crecimiento de las noticias falsas es hoy en día una realidad creciente, que lleva a los usuarios a sentirse inseguros cuando consumen información. Las noticias basadas en texto son quizás las más manipuladas, pero el vídeo está ganando terreno rápidamente. La tecnología permite adulterar fácilmente los contenidos, lo que lleva a los usuarios a estar mal informados. En este estudio se explican las diferentes técnicas de manipulación de imagen, vídeo y audio que se llevan a cabo con software y técnicas audiovisuales avanzadas. Los métodos más destacados son el morphing *y el* warping*, junto con las técnicas de aprendizaje automático. Además, la inteligencia artificial es un elemento crítico en el crecimiento de la generación de vídeos falsos. Esto conlleva la necesidad de identificar los vídeos falsos para verificar los hechos que se cuentan. También es esencial entender la tolerancia social, especialmente en los programas de humor, ya que algunos medios de comunicación utilizan estos mecanismos. Además, se analiza la importancia de las políticas de privacidad que afectan a la recogida de información personal de los usuarios y sus implicaciones en sus derechos fundamentales. Finalmente, se concluye con la necesidad de realizar campañas de alfabetización mediática y digital en el sistema educativo para minimizar este problema.*

Palabras clave

Deepfake, desinformación, manipulación de vídeos, apps, aplicaciones móviles.

1. Introduction

The generation of fake news, in text, image and video formats, seems to increase daily, reaching such levels that citizens can, at times, face difficulties in being correctly informed about what is going on in the world. Relevant examples include the transmission via instant messaging applications of hoax information related to the appearance of COVID-19 (Atehortua and Patino, 2021) and the generation of disinformation from Macedonia about the 2016 US presidential elections (Hughes and Waismel-Manor, 2021).

Fake news is mostly textual; however, images or videos can also be manipulated. These *deepfakes*, as they have come to be known, can be defined as the generation of deliberately misleading or false audiovisual content by manipulating images, sound and video. They are further characterised by the fact that this content is decontextualized in terms of time, form and place.

Both fake news and deepfakes are created with a similar goal in mind: the deception of the user. Yet, because it is clearly much easier for the user to process visual information than other types of information, manipulated images have the potential to be much more viral. Indeed, the impact that a manipulated and decontextualized image or video might have is likely to be much greater than that of a text. For example, they can cause a journalist to commit an error when reporting a news story, which means reporters must be constantly aware of this danger and always corroborate carefully their sources of information (Joseph, 2019).

Deepfakes integrate different types of content (image, video, and audio) which when woven together allow fake videos to be created. These deepfakes aim to deceive the user by manipulating, for example, a character or by using techniques of animation. In this way, customisations can be created by exploiting audiovisual technology at a range of different levels, including, for example, the face, the voice, the lip movement and the head and body posture. Although there are mobile applications that allow deepfakes to be generated very cheaply, the creation of professional videos – those that really deceive the public – is costly since it requires the participation of experts from different fields, including linguists, video editors, and animators, among others. For this reason, the production of deepfakes tends to be associated with much more elaborate objectives than those of simple satire or jokes. In an extreme case, a video created using these techniques could lead to a candidate standing for and winning an election.

In the news media, there are mechanisms that can help identify manipulated information. In the case of fake news, verification filters are used for fact-checking. In the case of deepfakes, biometric analysis or blockchain technology is used (Hasan and Salah, 2019); however, it should be noted that their application is costly in the extreme.

For technical reasons, it is much less difficult to modify a photograph than a video. The image is static and lacks elements that form part of a person's physiognomy or anatomy, such as their voice or movement. In the case of the manipulation of video, additional difficulties have to be overcome, including those of resolution, digital format and its runtime. In the case of image manipulation, different techniques have traditionally been used, perhaps the best known being the *morphing* technique that emerged in the 70s as applied in aeronautical applications. This involves modifying an image by means of metamorphosis via which image A can be transformed into image B and vice versa (Ivakhiv, 2016). This technique allows, for example, one face to be changed for another, integrating the face of one person onto another, or for caricatures to be created by exaggerating facial features.

In the video world, artificial intelligence has originated more advanced technology so that it is possible not only to change a person's physiognomy but also to integrate other characteristics, including the voice and lip movement. However, this technique still runs into a number of technical barriers as is evident in the video created by *Future Advocacy and UK Artist Bill Posters* in which Boris Johnson and Jeremy Corbyn endorse each other's candidacies to be UK Prime Minister (BBC News, 2019), a video that serves as an example of how such a vital factor as democracy itself can be undermined. The use of such videos and manipulated photographs in an informative context, such as the news, could mean that they are not perceived as fake precisely because of the prestige of the news media outlet.

If we start from the basic fact that the objective of fake news – which today continues to be primarily textual – is to deceive the user, then the objective of deepfakes cannot be said to differ greatly. Indeed, the decontextualization of a video or an image can also be classified as fake news, although in this article our focus is more specifically on the artificial manipulation of video.

A video piece can incorporate images, video or audio. This set of elements when woven together allows a fake video to be created; however, even if treated separately they can constitute part of a deepfake video. Therefore, as regards their morphology, deepfakes can include false footage, images, audio as well as video. Conceptually, a deepfake seeks to deceive the user through character customisation or by means even of animation. The customisation that is achieved with audiovisual technology involves manipulation of certain characteristics of a person, including their face, voice, lip movement and even their cloning (Khodabakhsh et al., 2018). Satire, which exists in a textual format, can also be represented in an audiovisual object such as video. However, in the production of deepfakes, there is one factor whose influence is especially marked: the economic cost. Although there are apps that allow deepfakes to be generated cheaply, creating videos that genuinely deceive is expensive.

From the point of view of the end user, the generation of fake images and even fake videos is becoming easier, since it is possible to find both desktop computer programs and apps that allow a person's physiognomy to be modified, especially the face by morphing one into another. This reduces the obstacles to the generation of false images. Likewise, computerized and more complex versions can be found that use machine-learning algorithms to create computer-generated faces (BBC News, 2018).

In the following sections, different aspects that directly or indirectly impact the implications of deepfakes are analysed. The specific domains examined are techniques of image and video manipulation, mechanisms for detecting manipulated videos, social tolerance of video manipulation, and the importance of privacy policies.

2. Techniques of image, audio and video manipulation

The principal technique used for manipulating images or videos is, as we have seen, *morphing*, consisting of the identification of patterns between two photographs and the dynamic transformation of one image into another with movement as it shifts from point A to point B (Ivakhiv, 2016; Scherhag et al., 2017). The technique has had a wide range of applications, one use being in major cinema productions, including *Indiana Jones and the Last Crusade*, which was one of the first films to use it (Puerto, 2018). In the field of psychology, the *morphing* technique is used to help in the perception of identity and different types of expression (Kramer et al., 2017). As the technology has evolved and as its results have improved, the technique has incorporated elements of 3D, for example, in facial expressions (Tang and Ni, 2019).

Another of the current techniques in use is *warping*, which allows the shape of some part of the image to be digitally modified for creative purposes, correcting possible dysfunctions or even creating distortions (Prathap et al., 2016). This technique has different applications including the generation of caricatures by way of the exaggeration of personal features. The technique is also used in the field of healthcare in radiotherapy (Veiga et al., 2015) and in photography to correct panoramic images in sports cameras (Li et al., 2015). Finally, *warping* is used for the post-production of images, and is commonly used for aesthetic enhancements of photos on social media (Islam et al., 2017; Krylov et al., 2014).

In the case of audio manipulation, different techniques are also being exploited and include, for example, voice exchange based on text-to-speech technology, which allows the audio in a recording to be changed and a new text to be rewritten (Cole, 2019; Somers et al., 2006; Wijethunga et al., 2020).

When audio and video manipulation are combined, another technique is used, that of lip-syncing, which involves modifying the movements of the speaker's mouth to match the fake words. This technique is used when a person is speaking and the camera shot focuses solely on them, in what is known as a *talking-head* video (Kietzmann et al., 2020). The technique is also used, for example, in the modeling of 3D video games (Ali et al., 2018).

Therefore, different techniques are available that facilitate total or partial changes to be made to a person's physiognomy, making it easier for deception to occur.

3. Detection of manipulated videos

Just as there are tools to detect fake news texts, tools have been developed to detect fake videos. These tools are high-tech in their specifications and have been developed at high costs. Joseph (2019) points out that the term deep fake, a portmanteau of "deep learning" and "fake", involves the application of machine learning and artificial intelligence techniques aimed at generating videos showing people saying or doing things that they have never said or done. Various mechanisms exist to detect fake videos without having to use a specific technological tool. For example, conducting an internet search to see if someone else is reporting on the content of a video, taking screen grabs and conducting reverse image searches to try to find the original or using verified trusted sources of information.

To use technology to identify fake videos, several methods are available. The use of recurrent neural networks where inconsistencies between video frames are used to detect whether or not a video has been manipulated (Güera and Delp, 2018). Big data analysis made it possible to detect that many fake videos employed faces that did not blink, and so fake video detection software was developed based on this fact (Li, Chang, and Lyu, 2018). There is also the option of performing a multimedia forensic analysis as a way to ensure the authenticity of a video and its origin (Rossler et al., 2019).

Although there is no definitive solution for detecting a fake video manipulating a person, the key is to develop tools that can go some way in helping to identify possible deepfakes (Nguyen et al., 2019). Analyses using methods based on automatic-learning and machine-learning algorithms can also provide solutions, such as image frequency analysis that helps to recognise different behaviours within a video. In short, the use of cutting-edge technologies can assist in the detection of fake videos.

4. Social tolerance of video manipulation

There are certain social domains in which modifications of a person's anatomy using different graphic techniques are tolerated and even accepted – examples include simulations of the outcomes of cosmetic surgery, as well as for the purposes of humour and satire – and where fake videos are professionally generated.

In the case of cosmetic surgery or other applications in the field of healthcare, there are various justifications for creating video simulations. Both female and male facial features can have a bearing on physical attraction and this fact has generated considerable demand for such simulations (Foo et al., 2017). Thus, in plastic surgery, a prospective patient's expectations regarding the outcomes can be increased by the exploitation of fake before-and-after testimonies from patients that have undergone operations (Crystal et al., 2020).

In the case of videos created for the purposes of parody or satire, it should be borne in mind that in some countries they are subject to specific legislation. Copyright laws also determine whether or not these videos can be made. One well-known case was the release of a video parodying former UK Prime Minister David Cameron, showing him 'rapping' a speech to the rhythms of hip-hop at a Conservative Party Conference. Thanks to legislative changes in copyright in the UK, the video could be published on YouTube, where it attracted millions of views (Baker, 2014). It should also be noted that satire and fake news have a different narrative. While in fake news or deepfakes, the objective is to deceive, in satire, the objective is to criticise someone from a position where the full informational context is available (Das & Clark, 2019).

In the audiovisual sector, there seems to be a degree of social tolerance for fake videos used for humour. An example of this is provided by the programme "*El Intermedio*", broadcast on the Spanish television network La Sexta (La Sexta, 2019), in which the manipulation of videos is very much part and parcel of the programme. Videos are shown in which previous interventions of politicians, actors and sportsmen and women are manipulated, putting fake words into their mouths with a humorous slant on some topical news story or other.

Radio stations, too, transmit programmes of humour in which the voice of a person is imitated or changed. Applying voice synthesis technology facilitates this type of programme, but it also allows fake news to be created (Stark, 2016). However, while humour is accepted in the media, especially the radio, the protection of the basic rights of individuals is an issue that needs to be carefully reflected on (Bendel, 2019).

Other cases have also come to light in which, for example, the manipulation of videos in the tourism sector have been used to help promote a tourist destination and influence an area's economy (Kwok and Koh, 2021), although the authors of this particular study acknowledge that it is an aspect that has yet to be explored in much depth.

Thus, we identify situations in which the creation of manipulated videos has become democratized and socially accepted, despite the fact their effects can be both positive and negative. However, we should not forget that reality is being distorted with all the potential dangers that this might entail.

5. The importance of privacy policies

As discussed above, smartphone applications have been developed to generate deepfakes. Such apps are covered by privacy policies, however, that do not always fulfil their function, namely to inform customers about how the application handles and processes the personal information they provide it with. Indeed, many apps share information with third parties and users should be informed of this fact. This occurs because applications tend to use third-party software, in many cases libraries, regarding which little is known as to what personal data they collect since the libraries fail to indicate what information is saved (Balebako et al., 2014).

Moreover, these policies are not always clear and, in some cases, can put the user's individual reputation at risk and even, in some instances, impact their health (Parker et al., 2019). The authors of this last study carried out an analysis of 61 mental health apps, and found that 41% of the apps analysed did not have privacy policies to inform users about how and when their personal data were collected and shared with third parties.

Similarly, in a study conducted in India, also in the field of health, a total of 70 apps were analysed, comparing the complexity involved in the reading of privacy policies for apps linked to mental health and diabetes (Powell et al., 2018). The study concluded that the privacy policies were written for users with a university level of education and that this complexity in the interpretation could be a barrier for decision making. In another study carried out on 369 mental health apps, it was determined that the information in their privacy policies was not transparent enough for users, that they were too generic and required a level of university literacy to be understood (Robillard et al., 2019).

Another of the problems associated with apps is their incorrect documentation, which can generate a considerable lack of confidence among users. Yu et al. (2016) conducted a study of the trustworthiness of the privacy policies of mobile applications. To do this, they adopted a systematic approach employing a system they named *PPChecker* which, by means of natural language processing techniques, allowed them to dissect the apps' privacy policies, focusing on three types of problem: a) incomplete privacy policies, b) incorrect privacy policies and c) inconsistent privacy policies. In their study, they analysed 1,197 apps and found that 282 (23.6%) presented at least one of these three problems, and that 222 (18.5%) had incomplete privacy policies.

To address this problem, Yu et al. (2017) developed novel software, named AutoPPG, to automatically construct and write correct and readable descriptions and so facilitate the generation of privacy policies for smartphone applications. To do this, they compared 20 privacy policies randomly selected from the sample of 7,781 applications used in their study. They found that AutoPPG tended to reveal more operations related to users' personal data than actually appeared in the existing privacy policies.

Zimmerle and Wall (2019) have drawn up a set of guidelines for the evaluation of privacy policies in mobile applications for children, as well as for children's websites. The authors define the key elements that should be included in privacy policies: a description of all personal data collected; details of the use that third parties can make of the information collected; specification of the parental control options that parents/guardians can implement; and, finally, a highly visible link to the privacy policies.

6. Conclusions

There are many issues that need to be addressed in relation to mobile applications, and not only those that allow the manipulation of images to generate deepfakes, but also in relation to all other types of application.

In the case of manipulation techniques, such as morphing, it is possible that, with the development of new algorithms and more innovative technological processes, it will be possible to improve the process of changing a person's physiognomy, which is the key to producing deepfakes. Future advances in artificial intelligence and machine learning look set to facilitate these changes.

Likewise, the detection of manipulated videos will become increasingly complex as well as more efficient, given that the same advances permitting the modification of a video will also be used in the detection of falsifications. However, there will always be a certain time lag in this regard. And this may be enough to make other types of audiovisual manipulations.

The application of privacy policies is a complex issue and not solely because their global distribution leads to problems of legislative jurisdiction. There are also inconsistencies in the information offered to users about the data collected and shared by the application. Perhaps the creation of a standard could make it easier for privacy policies to be more consistent with the operations that apps actually perform.

To conclude, it is critical that steps be taken to ensure that in all areas, not only in the academic arena and schools, that people are made aware of the need to prevent the development and use of deepfakes. Digital and media literacy campaigns are now more essential than ever in our rapidly changing digital world.

References

Ali, I. R., Kolivand, H., y Alkawaz, M. H. (2018). Lip syncing method for realistic expressive 3D face model. *Multimedia Tools and Applications*, 77(5), 5323–5366. https://doi.org/10.1007/s11042-017-4437-z

Atehortua, N. A., y Patino, S. (2021). COVID-19, a tale of two pandemics: Novel coronavirus and fake news messaging. *Health Promotion International, 36*(2), 524–534. https://doi.org/10.1093/heapro/daaa140

Baker, V. (2014). Humour on record: Why parody videos need to be protected. *Index on Censorship, 43*(4), 134-136. https://doi.org/10.1177/0306422014560520

Balebako, R.; Marsh, A.; Lin, J., Hong, J. & Cranor, L. (2014). The Privacy and Security Behaviors of Smartphone App Developers. *Figshare. Journal contribution.* https://doi.org/10.1184/R1/6470528.v1

BBC News (March 1, 2018). Deepfakes: The Face-Swapping Software. *BBC News.* https://www.bbc.com/news/av/technology-43118477/deepfakes-the-face-swapping-software-explained

BBC News (November 12, 2019). Are You Fooled by This Johnson-Corbyn Video? *BBC News.* https://www.bbc.com/news/av/technology-50381728/the-fake-video-where-johnson-and-corbyn-endorse-each-other

Bendel, O. (2019). The synthetization of human voices. *AI & Society, 34*(1), 83–89. https://doi.org/10.1007/s00146-017-0748-x

Cole, S. (April 26, 2019). A Site Faking Jordan Peterson's Voice Shuts Down After Peterson Decries Deepfakes. *Vice.com.* https://www.vice.com/en/article/43kwgb/not-jordan-peterson-voice-generator-shut-down-deep-fakes

Crystal, D. T.; Cuccolo, N. G.; Ibrahim, A. M. S.; Furnas, H. & Lin, S. J. (2020). Photographic and video deepfakes have arrived: How machine learning may influence plastic surgery. *Plastic and Reconstructive Surgery, 145*(4), 1079–1086. https://doi.org/10.1097/PRS.0000000000006697

Das, D. & Clark, A. J. (2019). Satire vs fake news: You can tell by the way they say it. 22-26. *In First International Conference on Transdisciplinary AI, TransAI,* (pp. 22-26). https://doi.org/10.1109/TransAI46475.2019.00012

Foo, Y. Z.; Simmons, L. W. & Rhodes, G. (2017). Predictors of facial attractiveness and health in humans. *Scientific Reports,* 7(1), 39731. https://doi.org/10.1038/srep39731

Güera, D. & Delp, E. J. (2018). Deepfake video detection using recurrent neural networks. In *15th IEEE International Conference on Advanced Video and Signal Based Surveillance, AVSS*, (pp. 1–6). https://doi.org/10.1109/AVSS.2018.8639163

Hasan, H. R. & Salah, K. (2019). Combating deepfake videos using blockchain and smart contracts. *IEEE Access*, (7), 41596–41606. https://doi.org/10.1109/ACCESS.2019.2905689

Hughes, H. C. & Waismel-Manor, I. (2021). The macedonian fake news industry and the 2016 US election. PS: *Political Science & Politics, 54*(1), 19–23. https://doi.org/10.1017/S1049096520000992

Islam, M. B.; Lai-Kuan, W. & Chee-Onn, W. (2017). A survey of aesthetics-driven image recomposition. *Multimedia Tools and Applications, 76*(7), 9517–9542. https://doi.org/10.1007/s11042-016-3561-5

Ivakhiv, A. (2016). The Art of Morphogenesis: Cinema in and beyond the Capitalocene. In: Shane Denson, J. L. (Hg.): *Post-Cinema. Theorizing 21st-Century Film*, (pp. 724-749). REFRAME Books. https://doi.org/10.25969/mediarep/13475

Joseph, R. (2019). Fakebusters strike back: How to spot deep fakes, the manipulated videos that are the newest form of "fake news" to hit the internet. *Index on Censorship, 48*(1), 76-79. https://doi.org/10.1177/0306422019841326

Khodabakhsh, A.; Busch, C. & Ramachandra, R. (2018). A taxonomy of audiovisual fake multimedia content creation technology. In *IEEE Conference on Multimedia Information Processing and Retrieval, MIPR*, (pp. 372–377). https://doi.org/10.1109/MIPR.2018.00082

Kietzmann, J.; Lee, L. W. ,McCarthy, I. P. & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons, 63*(2), 135-146. https://doi.org/10.1016/j.bushor.2019.11.006

Kramer, R. S. S.; Jenkins, R. & Burton, A. M. (2017). InterFace: A software package for face image warping, averaging, and principal components analysis. *Behavior Research Methods, 49*(6), 2002–2011. https://doi.org/10.3758/s13428-016-0837-7

Krylov, A.; Nasonova, A. & Nasonov, A. (2014). Image warping as an image enhancement post-processing tool. In Paulus, D.; Fuchs, C. & Droege, D. (ed.) *Proceedings of the 9th Open German-Russian Workshop on Pattern Recognition and Image Understanding*, (pp. 132-135). Universität Koblenz-Landau. https://kola.opus.hbz-nrw.de/frontdoor/index/index/docId/915

Kwok, A. O. J. & Koh, S. G. M. (2021). Deepfake: A social construction of technology perspective. Current Issues in Tourism, 24(13), 1798–1802. https://doi.org/10.1080/13683500.2020.1738357

La Sexta (2019). Videos Manipulados - *El Intermedio*. https://www.lasexta.com/programas/el-intermedio/videos-manipulados/

Li, D.; He, K.S, un, J. & Zhou, K. (2015). A geodesic-preserving method for image warping. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, CVPR*, (pp. 213–221). https://doi.org/10.1109/CVPR.2015.7298617

Li, Y.; Chang, M.-C. & Lyu, S. (2018). In ictu oculi: Exposing ai created fake videos by detecting eye blinking. In *IEEE International Workshop on Information Forensics and Security, WIFS*, (pp. 1–7). https://doi.org/10.1109/WIFS.2018.8630787

Nguyen, H. H.; Yamagishi, J. & Echizen, I. (2019). Use of a capsule network to detect fake images and videos. *ArXiv:1910.12467 [Cs]*. http://arxiv.org/abs/1910.12467

Parker, L.; Halter, V.; Karliychuk, T.& Grundy, Q. (2019). How private is your mental health app data? An empirical study of mental health app privacy policies and practices. *International Journal of Law and Psychiatry, 64*, 198–204. https://doi.org/10.1016/j.ijlp.2019.04.002

Powell, A.; Singh, P. & Torous, J. (2018). The complexity of mental health app privacy policies: A potential barrier to privacy. *JMIR MHealth and UHealth, 6*(7), e158. https://doi.org/10.2196/mhealth.9871

Prathap, K. S. V.; Jilani, S. A. K. & Reddy, P. R. (2016). A critical review on Image Mosaicing. In *International Conference on Computer Communication and Informatics, ICCCI*, (pp. 1–8). https://doi.org/10.1109/ICCCI.2016.7480028

Puerto, S. (2018). Técnicas de animación e interrelación de imágenes bidimensionales. *Mosaic*, 165. https://doi.org/10.7238/m.n165.1842

Robillard, J. M.; Feng, T. L.; Sporn, A. B.; Lai, J.-A.; Lo, C.; Ta, M. & Nadler, R. (2019). Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet Interventions*, 17, 100243. https://doi.org/10.1016/j.invent.2019.100243

Rossler, A.; Cozzolino, D.; Verdoliva, L.; Riess, C.; Thies, J. & Niessner, M. (2019). Faceforensics++: Learning to detect manipulated facial images. In *Proceedings of the IEEE/CVF International Conference on Computer Vision, ICCV*, (pp. 1–11). https://doi.org/10.1109/ICCV.2019.00009

Scherhag, U.; Nautsch, A.; Rathgeb, C.; Gomez-Barrero, M.; Veldhuis, R. N. J.; Spreeuwers, L.; Schils, M.; Maltoni, D.; Grother, P.; Marcel, S.; Breithaupt, R.; Ramachandra, R. & Busch, C. (2017). Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting. In *International Conference of the Biometrics Special Interest Group, BIOSIG*, (pp. 1–7). https://doi.org/10.23919/BIOSIG.2017.8053499

Somers, H.; Evans, G. & Mohamed, Z. (2006). Developing speech synthesis for under-resourced languages by «faking it»: An experiment with Somali. In *Proceedings of the Fifth International Conference on Language Resources and Evaluation, (pp.* 2578-2581). http://www.lrec-conf.org/proceedings/lrec2006/pdf/483_pdf.pdf

Stark, J. (September 11, 2016). Adobe stellt Sprach-Software Voco vor!-Das Computer-Magazin. *Com! Professional*. https://www.com-magazin.de/news/adobe-systems/adobe-stellt-sprach-software-voco-1146967.html

Tang, J. & Ni, B. (2019). Progressive face dynamic morphing. In *International Conference on Intelligent Computing, Automation and Systems, ICICAS*, (pp. 48–53). https://doi.org/10.1109/ICICAS48597.2019.00019

Veiga, C.; Lourenço, A. M.; Mouinuddin, S.; van Herk, M.; Modat, M.; Ourselin, S.; Royle, G. & McCle-

lland, J. R. (2015). Toward adaptive radiotherapy for head and neck patients: Uncertainties in dose warping due to the choice of deformable registration algorithm: Dose warping uncertainties due to registration algorithm. *Medical Physics, 42*(2), 760–769. https://doi.org/10.1118/1.4905050

Wijethunga, R. L. M. A. P. C.; Matheesha, D. M. K.; Noman, A. A.; De Silva, K. H. V. T. A.; Tissera, M. & Rupasinghe, L. (2020). Deepfake audio detection: A deep learning based solution for group conversations. In *2nd International Conference on Advancements in Computing, ICAC*, (pp. 192-197) https://doi.org/10.1109/ICAC51239.2020.9357161

Yu, L.; Luo, X.; Liu, X. & Zhang, T. (2016). Can We Trust the Privacy Policies of Android Apps? In *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN*, (pp. 538-549). https://doi.org/10.1109/DSN.2016.55

Yu, L.; Zhang, T.; Luo, X.; Xue, L. & Chang, H. (2017). Toward Automatically Generating Privacy Policy for Android Apps. *IEEE Transactions on Information Forensics and Security, 12*(4), pp. 865-880. https://doi.org/10.1109/TIFS.2016.2639339

Zimmerle, J. C. & Wall, A. S. (2019). What’s in a policy? Evaluating the privacy policies of children’s apps and websites. *Computers in the Schools, 36*(1), 38–47. https://doi.org/10.1080/07380569.2019.1565628