

# A survey of deepfakes in terms of deep learning and multimedia forensics

Wildan Jameel Hadi<sup>1</sup>, Suhad Malallah Kadhem<sup>2</sup>, Ayad Rodhan Abbas<sup>2</sup>

<sup>1</sup>Department of Computer Science, College of Science for Women, Baghdad University, Bagdad, Iraq

<sup>2</sup>Department of Computer Science, College of science, Al-Technology University, Baghdad, Iraq

---

## Article Info

### Article history:

Received Jul 27, 20

Revised Feb 22, 2022

Accepted Apr 12, 2022

---

### Keywords:

Autoencoder

Deep learning

Deepfake

Generative adversarial network

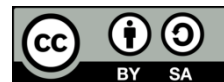
Multimedia forensics

---

## ABSTRACT

Artificial intelligence techniques are reaching us in several forms, some of which are useful but can be exploited in a way that harms us. One of these forms is called deepfakes. Deepfakes is used to completely modify video (or image) content to display something that was not in it originally. The danger of deepfake technology impact on society through the loss of confidence in everything is published. Therefore, in this paper, we focus on deepfake detection technology from the view of two concepts which are deep learning and forensic tools. The purpose of this survey is to give the reader a deeper overview of i) the environment of deepfake creation and detection, ii) how deep learning and forensic tools contributed to the detection of deepfakes, and iii) finally how in the future incorporating both deep learning technology and tools for forensics can increase the efficiency of deepfakes detection.

*This is an open access article under the [CC BY-SA](#) license.*



---

## Corresponding Author:

Wildan Jameel Hadi

Department of Computer Science, Baghdad University

Bagdad, Iraq

Email: wildanjh\_comp@cs.w.uobaghdad.edu.iq

---

## 1. INTRODUCTION

Artificial intelligence (AI) methods and algorithms help to provide solutions in many areas [1]–[4]. One of the categories of artificial intelligence is called machine learning. It is a type of statistical learning in which each item of the database is described by several characteristics or attributes. Machine learning models have been applied in many areas of research [5]–[9]. In contrast, the other category of AI claims deep learning, which is also a type of statistical learning but extracts feature from input data. Deep learning helped to create deepfakes. The term deepfake picked up its name from an unknown client of the platform Reddit, who passed by the name 'deepfakes' (deep learning + fakes) and who shared the first deepfakes by putting accidental big names of celebrities into porn clips [10]. Most of the deepfakes follow a method in which the real face of a certain person is replaced by a fake image of another person, as shown in the Figure 1.

Social media platforms are considered one of the platforms most targeted by deepfakes technology for easy spreading of rumors, lies and fabricated news. At the same time, 'infopocalypse' makes people trust any piece of information as it comes from their social networks that include close family members and friends. In fact, most people agree with anything that supports their views and preferences, even if they know it is fake. In recent times, high-quality realistic deep counterfeiting manufacturing resources are increasingly available as open source for creating deceptive operations. This prompts users with little skills to fitly create altered videos in terms of replacing faces, synthesizing speech, and changing expressions [11]. In example is fake Queen Elizabeth spoke on TV screens on christmas as part of a "deepfake" speech aired by Channel 4 in the U.K. There would a few reasons with accept deepfake disinformation could bring an impeding societal impact, which will be the reason examining impacts from claiming deepfake disinformation is worth those

experimental investigations. Firstly, deepfakes can make sensible disinformation. Automatically created sounds and images can be accepted as original images and sounds. A conventional resident might battle until recognize way from fiction. secondly, it is possible to use deepfake to increase malinformation by, for example, posting a fabricated video of Queen Elizabeth II's speech on any official occasion. Third, deepfakes might additionally make an manifestation about productive disinformation. Whether a political performer need enough preparation data, the on-screen character could make large portions different, sensible deepfakes of the same representative in a short time of time. On mix for political micro targeting (PMT) techniques, deepfakes have a chance to be particularly impactful. We are not there yet. Deepfakes don't yet surge people in a general sphere, let micro targeted deepfakes. Be that (micro targeted) deepfakes bring those aspects that make them conceivably precise capable modes for disinformation in the close to future [12]. From above, we note how dangerous this technology is and its impact on society, so it is very important to shed light on this technology and how to develop techniques in fingerprints, forensic science and verification techniques to detect fake video from the original. There are currently some methods used to detect fake video using deep learning techniques or traditional forensic tools, which will be mentioned in this survey, but in general, the tools that detect deep fakes remain in their early stages. So that, our contribution here is to see how the performance of the deepfake detector will increase if we are combined both concepts (deep learning + forensic tools) in the same model. Organization of the sections of this article is: section 2 shows how deepfakes is created methods for detecting deepfake in section 3. Finally, section 4 shows discussion and conclusion.



Figure 1. Example of deepfakes [13]

## 2. CREATION OF DEEPPFAKES

Deepfakes technology can be used as a synonym for any video or image that has been manipulated with the use of deep neural networks. This manipulation is not simple to perform on standard computers but requires high-end desktops with strong graphical cards or best still with computing capacity in the cloud. This minimizes the processing time required to train deep networks responsible for creating deepfakes. Deepfakes in terms of facial manipulation can be classified in the following categories [14]:

### 2.1. Face swap

Recently, face swap is the most common category of face manipulation. This is accomplished using one type of deep neural networks. This type is autoencoder, which is used in feature extraction and image compression [15]–[17]. Autoencoder (encoder + decoder) structure is used by Reddit user as the first trail of deepfake creation [18], [19]. The basic idea behind autoencoder is to represent the input data into a smaller, more compressed representation and then the ability to retrieve the original data from this medium representation. The process of creating deepfakes can be shown in Figure 2. Generally, this process requires training two autoencoders, each work on a set of video clips of one person from the two persons whose identities will exchange. After the autoencoders are trained, the target video is given to the wrong decoder to produce a deepfake face [20]. In general, deepfakes created using autoencoder make the swapped face look like the target face and the source face without paying much attention to the difference between the identity of both the source and the target faces. To produce more deep swapped faces, Yang *et al.* [21] combined Cross-identity adversarial in training.

### 2.2. Face synthesis

Generative adversarial networks (GANs) are used in this category to create non-existent real faces. The emergence of GANs helped to produce surprisingly realistic results that lead to the birth of deepfakes [22]. The most popular way is STYLEGAN (a special type of GANs) was used to output the seeming “this person does not exist” website [23]. Researches improve the capability of style GAN architecture and suggest a new a version – StyleGAN2 [24].

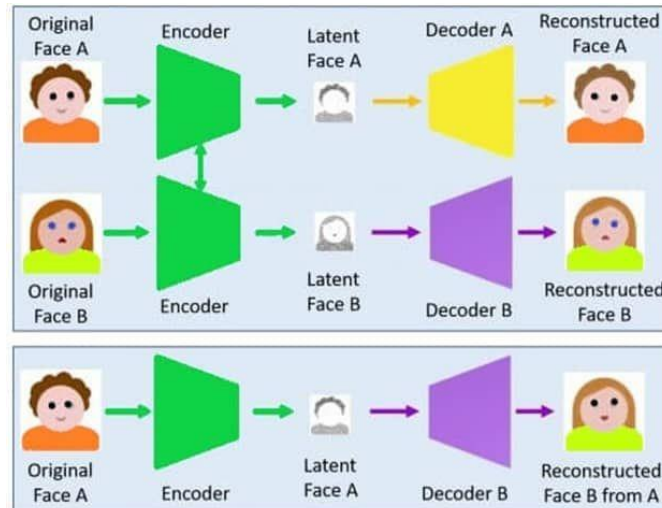


Figure 2. Deepfake creation process. Each autoencoder is trained on a set of images of one person

### 2.3. Facial attributes and expression

Deepfakes images can be generated by performing facial expression and attributers manipulation such as modifying the skin color, the gender, the age, and the face expression. To perform this image to image translation GANs also used. The best method applied for this purpose is STARGAN (a special type of GANs) [25]. For facial expression manipulation, Bodur *et al.* [26] proposed an end to end deep network. They use two generative adversarial networks (RGB network + depth network) to translate the source RGB image to a given target label.

## 3. DEEPFAKE DETECTION

### 3.1. Deep learning based methods

As a result of the effect of deepfake technology on many areas, research papers in the last two years have become directed towards this technology and explain all the challenges and techniques related to it [27]. Usually, images resulting from the application of deepfake algorithms often need more transformation to fit the area to be forged in the source video. Such transformations leave distinct defects. Here comes the role of deep learning networks to detect these defects. Li and Lyu [28] trained four models of convolution neural network (CNN): residual networks (ResNet152, ResNet10, ResNet50) [29], and VGG16 (stands for visual geometry group) [30]. The result CNN model architecture strongly distinguish real videos from tampered ones. In [31] a generalized CNN model is developed to increase its capability to detect a different manipulation but related to the origin. To reduce the number of parameters required for traditional CNN, capsule networks are used in [32] to build a light weight detection system.

Instead of using visual artifacts within a frame, the temporal features also can be used in deepfake detection. The discrepancies among video frames can be discovered using recurrent neural network (RNN) [33]. Analysis of two steps are proposed by [34] consist of extracting frame features using CNN followed by recognizing temporal conflict between frames due to the process of face swapping as shown in Figure 3.

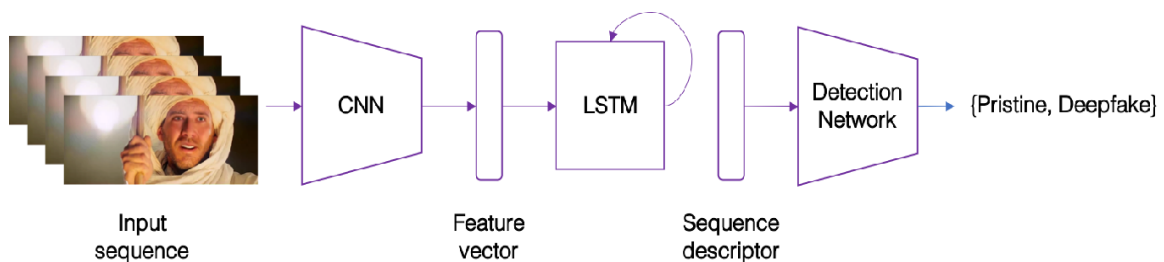


Figure 3. Firstly, CNN is used for extracting frame features and then fed to long short-term memory (LSTM) for analyzing them

Eye blinking also can provide a good point in detecting fake videos, because this rate in the fake videos may be fewer or higher than the eye blinking rate in real ones. Li *et al.* [35] use a combination of CNN model and recursive neural network to produce long term recurrent CNN (LRCN) [36], for detecting the motion of eyelid. Spatial-temporal will be also utilized within data analysis. The point when information is gathered over both space also time. Nguyen *et al.* [37] could take spatio-temporal characteristics from a contiguous frame sequence and learn them using a 3-D CNN network model to achieve over 99% as deepfake detection accuracy. Dynamic prototype network (DPNet) a powerful result that uses dynamic representations. (i.e., prototypes) will clarify deepfake temporal artifacts [38]. Specifically, DPNet's job includes focusing on temporal inconsistencies by learning its prototyping representations within the latent space, and then build predictions depending on how a test video dynamics are similar to the learned dynamic prototypes. Two-stream convolutional neural network (TwoStreamNet) proposed in [39]. The two networks recognize frequency and spatial domain artifacts separately, and then the output is fed to the end of the network for classification. Table 1 shows the summary of the above methods with their results. Finally detecting fake news using deep learning also has a stake in new research [40]–[43].

Table 1. Summary of most methods used for deepfake detection using deep learning

Author	DNN model	Basic idea	Dataset used
Li and Lyu [28]	CNN	Four CNN models are used to detect artifacts between the face area in fake video and its surrounding regions.	-UADFV from [27] consists of 49 fake videos and 49 real videos respectively. -TIMIT deepfake video dataset [44] having two sets of fake videos with different resolutions and equality.
Cozzolino <i>et al.</i> [31]	CNN	Achieve such generalization by developing CNN model.	Face Forensics data set [45].
Güera and Delpb [34]	CNN + RNN	-CNN network for frame level feature extraction. -The features extracted in step 1 are used for training RNN.	Dataset having approximately 300 videos collected from different websites plus 300 videos are chosen randomly from HOHA dataset [46].
Li <i>et al.</i> [35]	CNN + RNN	-Crop eye area from frame sequences. -Passing the cropped eye area sequences to LRCN (which includes three parts: feature extraction using CNN, sequence learning, and finally state prediction stage)	eye blinking video (EBV) dataset.
Nguyen <i>et al.</i> [32]	Capsule - Forensics	Firstly preprocessing step is applied to the input image and then passes to a part of the VGG19 network [47]. Before entering to capsule network VGG19 network pre-trained on ILSVRC database [48]. Finally, post-processing step, which works in agreement with the pre-processing one.	Face Forensics database [45].
Trinh <i>et al.</i> [38]	Dynamic Prototype Network (DPNet)	-Focusing on temporal inconsistencies by learning its prototyping representations within the latent space, -and then build predictions depending on how a test video dynamics are similar to the learned dynamic prototypes.	- Face Forensics++ [45] for training. -For testing four data set are used :1) Face Forensics++ [45]; 2) DeepfakeDetection [49]; 3) DeeperForensics-1.0 [50]; 4) Celeb-DF [51].
Yousaf <i>et al.</i> [39]	Two-stream CNN	The two network streams take frequency and spatial domain artifacts separately, and their outputs are fed to the end of the network for classification.	-For training, a data set of fake images generated by ProGAN [52] is used. -For testing a data set of fake images generated by other GANs.

### 3.2. Multimedia forensics based methods

This section reviews some ideas of the latest research in multimedia forensics. Detecting whether the multimedia content (video, audio, or image) is fake or not, different methods used to expose defects or anomalies in the multimedia content [53]–[55]. One of these exploitable anomalies is manufacturing defects, in which sensor elements deviate from their expected behavior. These deviations form a pattern that is likened to noise called photo-response non-uniformity (PRNU) noise. It is often known as the fingerprint of the digital image [56]. Rodriguez *et al.* [57] used this noise pattern in detecting the deepfake. Pu *et al.* [58] proposed a method for deepfake detection called it noise scope which consists of four main parts: noise extractor, fingerprint extractor, fingerprint classifier, and finally fake image detector. This method detects deepfake in a blind way i.e. the detector has no information about the generative model used and access only to real data. The accuracy of this method reaches about 99.68% in detecting GAN images. A new approach to detect deepfake is proposed by [59] based on the “JPEG ghost” algorithm. This algorithm recognizes tampered faces from real ones by analyzing incompatible compression errors.

### 3.3. Multimedia forensics and deep learning based methods

The Deepfake technique having a detrimental effect on people and society if it not controlled in time. It is a kind of exploitation of artificial intelligence methods and machine learning technology for unlawful purposes, such as incitement against a certain party or a public figure by creating the illusion that a person said something, and in fact, it is not. These changes are not noticeable to the eye of the recipient. Forces him to believe in her [13]. Before the occurrence of deep learning methods, forensic tools have long been considered to automatically detect tampering at physical, digital, and semantic levels [60]. Recently, deep learning has become of great interest by researchers, as it has the ability to learn features directly from the data [53].

Detection methods are still in their early stages and many challenges they face. So why do we not exploit the advantages of multimedia forensic methods and deep learning methods to get algorithms more robust in terms of detecting deepfakes?. For example, detecting different ratios of image compression using error level analysis followed by using the CNN model increases the detection accuracy [61]. This is because images with JPEG formats have the same compression level, so manipulation applied to that image will disturb the pressure levels between the modified area and the surrounding areas. Also, Habeeba *et al.* [62] proposed a two-step verification method, that used a three-layer neural network (NN) for fake video classifying and followed by a second confirmation step which includes a comparison of the laplacian variance for different patches in the face. They achieve good results in terms of accuracy and computational requirements.

## 4. CONCLUSION

In general, the quality of deepfakes technology is greatly increasing, so it is necessary to pay attention to methods of detecting deepfakes and increasing their strength. In this survey, we focused on showing the deepfakes environment. The methods used to detect deepfakes were also explained from two viewpoints (deep learning + multimedia forensics). we provided a brief view of these two concepts and how combining them increases the deepfakes detection accuracy. Finally, we hope this information is useful to the community in understanding and preventing malignant deepfakes.

## REFERENCES

- [1] A. T. S. Al-Obaidi, H. S. Abdullah, and Z. O. Ahmed, "Camel herds wlgorithm: a new swarm intelligent algorithm to solve optimization problems," *International Journal on Perceptive and Cognitive Computing*, vol. 3, no. 1, May 2017, doi: 10.31436/ijpcc.v3i1.44.
- [2] J. K. Alwan, A. J. Hussain, D. H. Abd, A. T. Sadiq, M. Khalaf, and P. Liatsis, "Political Arabic articles orientation using rough set theory with sentiment lexicon," *IEEE Access*, vol. 9, pp. 24475–24484, 2021, doi: 10.1109/ACCESS.2021.3054919.
- [3] T. Dewi, S. Nurmaini, P. Risma, Y. Oktarina, and M. Roriz, "Inverse kinematic analysis of 4 DOF pick and place arm robot manipulator using fuzzy logic controller," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 1376–1386, Apr. 2020, doi: 10.11591/ijece.v10i2.pp1376-1386.
- [4] A. T. Sadiq, M. G. Duaimi, and S. A. Shaker, "Data missing solution using rough set theory and swarm intelligence," in *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, Nov. 2012, pp. 173–180., doi: 10.1109/ACSAT.2012.29.
- [5] T. A. Assegie and P. S. Nair, "Handwritten digits recognition with decision tree classification: a machine learning approach," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 4446–4451, Oct. 2019, doi: 10.11591/ijece.v9i5.pp4446-4451.
- [6] D. H. Abd, A. T. Sadiq, and A. R. Abbas, "Political articles categorization based on different naïve bayes models," in *Communications in Computer and Information Science*, Springer International Publishing, 2020, pp. 286–301., doi: 10.1007/978-3-030-38752-5\_23.
- [7] A. R. Abbas and A. O. Farooq, "Human skin colour detection using bayesian rough decision tree," in *Communications in Computer and Information Science*, Springer International Publishing, 2018, pp. 240–254., doi: 10.1007/978-3-030-01653-1\_15.
- [8] D. H. Abd, A. T. Sadiq, and A. R. Abbas, "Classifying political arabic articles using support vector machine with different feature extraction," in *Communications in Computer and Information Science*, Springer International Publishing, 2020, pp. 79–94., doi: 10.1007/978-3-030-38752-5\_7.
- [9] A. L. H. P.S and U. Eranna, "A simplified machine learning approach for recognizing human activity," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 3465–3473, Oct. 2019, doi: 10.11591/ijece.v9i5.pp3465-3473.
- [10] S. Suwajanakorn, S. M. Seitz, and I. Kemelmacher-Shlizerman, "Synthesizing obama: learning lip sync from audio," *ACM Transactions on Graphics*, vol. 36, no. 4, pp. 1–13, Jul. 2017, doi: 10.1145/3072959.3073640.
- [11] L. Verdoliva, "Media forensics and DeepFakes: an overview," *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 910–932, Aug. 2020, doi: 10.1109/JSTSP.2020.3002101.
- [12] M. Westerlund, "The emergence of Deepfake technology: a review," *Technology Innovation Management Review*, vol. 9, no. 11, pp. 39–52, Jan. 2019, doi: 10.22215/timreview/1282.
- [13] T. Dobber, N. Metoui, D. Trilling, N. Helberger, and C. de Vreese, "Do (microtargeted) deepfakes have real effects on political attitudes?," *The International Journal of Press/Politics*, vol. 26, no. 1, pp. 69–91, Jan. 2021, doi: 10.1177/1940161220944364.
- [14] I. Korshunova, W. Shi, J. Dambre, and L. Theis, "Fast face-swap using convolutional neural networks," in *2017 IEEE International Conference on Computer Vision (ICCV)*, Oct. 2017, pp. 3697–3705., doi: 10.1109/ICCV.2017.397.
- [15] Z. Fan, D. Bi, L. He, M. Shiping, S. Gao, and C. Li, "Low-level structure feature extraction for image processing via stacked




- sparse denoising autoencoder,” *Neurocomputing*, vol. 243, pp. 12–20, Jun. 2017, doi: 10.1016/j.neucom.2017.02.066.
- [16] L. Zhou, C. Cai, Y. Gao, S. Su, and J. Wu, “Variational autoencoder for low bit-rate image compression,” in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2018, vol. 2018-Janua, pp. 2617–2620.
- [17] Z. Cheng, H. Sun, M. Takeuchi, and J. Katto, “Deep convolutional autoencoder-based lossy image compression,” in *2018 Picture Coding Symposium (PCS)*, Jun. 2018, pp. 253–257., doi: 10.1109/PCS.2018.8456308.
- [18] H. Vyas, “Deep fake creation by deep learning,” *International Research Journal of Engineering and Technology*, pp. 960–963, 2020
- [19] R. Katarya and A. Lal, “A study on combating emerging threat of deepfake weaponization,” in *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Oct. 2020, pp. 485–490., doi: 10.1109/I-SMAC49090.2020.9243588.
- [20] J. Pu *et al.*, “Deepfake videos in the wild: analysis and detection,” in *Proceedings of the Web Conference 2021*, Apr. 2021, pp. 981–992., doi: 10.1145/3442381.3449978.
- [21] S. Yang, H. Xue, J. Ling, L. Song, and R. Xie, “Deep face swapping via cross-identity adversarial training,” in *International Conference on Multimedia Modeling*, 2021, pp. 74–86., doi: 10.1007/978-3-030-67835-7\_7.
- [22] L. Guamera, O. Giudice, and S. Battiato, “Fighting deepfake by exposing the convolutional traces on images,” *IEEE Access*, vol. 8, pp. 165085–165098, 2020, doi: 10.1109/ACCESS.2020.3023037.
- [23] T. Karras, S. Laine, M. Aittala, J. Hellsten, J. Lehtinen, and T. Aila, “Analyzing and improving the image quality of StyleGAN,” in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Jun. 2020, pp. 8107–8116., doi: 10.1109/CVPR42600.2020.00813.
- [24] P. Zhu, R. Abdal, Y. Qin, J. Femiani, and P. Wonka, “Improved styleGAN embedding: where are the good latents?,” *arXiv:2012.09036*, Dec. 2020
- [25] Y. Choi, M. Choi, M. Kim, J.-W. Ha, S. Kim, and J. Choo, “StarGAN: unified generative adversarial networks for multi-domain image-to-image translation,” in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, Jun. 2018, pp. 8789–8797., doi: 10.1109/CVPR.2018.00916.
- [26] R. Bodur, B. Bhattarai, and T.-K. Kim, “3D dense geometry-guided facial expression synthesis by adversarial learning,” in *2021 IEEE Winter Conference on Applications of Computer Vision (WACV)*, Jan. 2021, pp. 2391–2400., doi: 10.1109/WACV48630.2021.00244.
- [27] D. Gong, “Deepfake forensics, an ai-synthesized detection with deep convolutional generative adversarial networks,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 2861–2870, Jun. 2020, doi: 10.30534/ijatcse/2020/58932020.
- [28] Y. Li and S. Lyu, “Exposing deepfake videos by detecting face warping artifacts,” *arXiv:1811.00656*, Nov. 2018
- [29] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Jun. 2016, pp. 770–778., doi: 10.1109/CVPR.2016.90.
- [30] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” *arXiv preprint arXiv:1409.1556*, Sep. 2014
- [31] D. Cozzolino, J. Thies, A. Rössler, C. Riess, M. Nießner, and L. Verdoliva, “ForensicTransfer: Weakly-supervised domain adaptation for forgery detection,” *arXiv:1812.02510*, Dec. 2018
- [32] H. H. Nguyen, J. Yamagishi, and I. Echizen, “Use of a capsule network to detect fake images and videos,” *arXiv:1910.12467*, Oct. 2019
- [33] W. M. Wubet, “The deepfake challenges and deepfake video detection,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 6, pp. 789–796, Apr. 2020, doi: 10.35940/ijitee.E2779.049620.
- [34] D. Guera and E. J. Delp, “Deepfake video detection using recurrent neural networks,” in *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, Nov. 2018, pp. 1–6., doi: 10.1109/AVSS.2018.8639163.
- [35] Y. Li, M.-C. Chang, and S. Lyu, “In Ictu Oculi: exposing AI created fake videos by detecting eye blinking,” in *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*, Dec. 2018, pp. 1–7., doi: 10.1109/WIFS.2018.8630787.
- [36] J. Donahue *et al.*, “Long-term recurrent convolutional networks for visual recognition and description,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 4, pp. 677–691, Apr. 2017, doi: 10.1109/TPAMI.2016.2599174.
- [37] X. H. Nguyen, T. S. Tran, V. T. Le, K. D. Nguyen, and D.-T. Truong, “Learning spatio-temporal features to detect manipulated facial videos created by the deepfake techniques,” *Forensic Science International: Digital Investigation*, vol. 36, Mar. 2021, doi: 10.1016/j.fsidi.2021.301108.
- [38] L. Trinh, M. Tsang, S. Rambhatla, and Y. Liu, “Interpretable and trustworthy deepfake detection via dynamic prototypes,” in *2021 IEEE Winter Conference on Applications of Computer Vision (WACV)*, Jan. 2021, pp. 1972–1982., doi: 10.1109/WACV48630.2021.00202.
- [39] B. Yousaf, M. Usama, W. Sultani, A. Mahmood, and J. Qadir, “Fake visual content detection using two-stream convolutional neural networks,” *arXiv:2101.00676*, Jan. 2021
- [40] S. R. Sahoo and B. B. Gupta, “Multiple features based approach for automatic fake news detection on social networks using deep learning,” *Applied Soft Computing*, vol. 100, Mar. 2021, doi: 10.1016/j.asoc.2020.106983.
- [41] A. Wani, I. Joshi, S. Khandve, V. Wagh, and R. Joshi, “Evaluating deep learning approaches for Covid19 Fake news detection,” in *arXiv:2101.04012*, 2021, pp. 153–163., doi: 10.1007/978-3-030-73696-5\_15.
- [42] J. A. Nasir, O. S. Khan, and I. Varlamis, “Fake news detection: A hybrid CNN-RNN based deep learning approach,” *International Journal of Information Management Data Insights*, vol. 1, no. 1, Apr. 2021, doi: 10.1016/j.ijime.2020.100007.
- [43] F. Gereme, W. Zhu, T. Ayall, and D. Alemu, “Combating fake news in ‘low-resource’ languages: Amharic fake news detection accompanied by resource crafting,” *Information*, vol. 12, no. 1, Jan. 2021, doi: 10.3390/info12010020.
- [44] P. Korshunov and S. Marcel, “DeepFakes: a new threat to face recognition? assessment and detection,” *arXiv:1812.08685*, Dec. 2018
- [45] A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, “FaceForensics: a large-scale video dataset for forgery detection in human faces,” *arXiv:1803.09179*, Mar. 2018
- [46] I. Laptev, M. Marszalek, C. Schmid, and B. Rozenfeld, “Learning realistic human actions from movies,” in *2008 IEEE Conference on Computer Vision and Pattern Recognition*, Jun. 2008, pp. 1–8., doi: 10.1109/CVPR.2008.4587756.
- [47] S. Shao, S. McAleer, R. Yan, and P. Baldi, “Highly accurate machine fault diagnosis using deep transfer learning,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 4, pp. 2446–2455, Apr. 2019, doi: 10.1109/TII.2018.2864759.
- [48] O. Russakovsky *et al.*, “ImageNet large scale visual recognition challenge,” *International Journal of Computer Vision*, vol. 115, no. 3, pp. 211–252, Dec. 2015, doi: 10.1007/s11263-015-0816-y.
- [49] “Fake-detection-dataset-for-deepfake-from-Google-and-Jigsaw.”
- [50] L. Jiang, R. Li, W. Wu, C. Qian, and C. C. Loy, “Deeper forensics-1.0: A large-scale dataset for real-world face forgery






- detection,” *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 2889–2898, Jan. 2020
- [51] Y. Li, X. Yang, P. Sun, H. Qi, and S. Lyu, “Celeb-df: A large-scale challenging dataset for deepfake forensics,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020, pp. 3207–3216.
- [52] T. Karras, T. Aila, S. Laine, and J. Lehtinen, “Progressive growing of gans for improved quality, stability, and variation,” *arXiv preprint arXiv:1710.10196*, 2017
- [53] D. Siegel, C. Kraetzer, S. Seidlitz, and J. Dittmann, “Media forensics considerations on DeepFake detection with hand-crafted features,” *Journal of Imaging*, vol. 7, no. 7, Jul. 2021, doi: 10.3390/jimaging7070108.
- [54] T. M. Shashidhar and K. B. Ramesh, “Novel framework for optimized digital forensic for mitigating complex image attacks,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 5, pp. 5198–5207, Oct. 2020, doi: 10.11591/ijece.v10i5.pp5198-5207.
- [55] T. M. Shashidhar and K. B. Ramesh, “Reviewing the effectivity factor in existing techniques of image forensics,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 6, pp. 3558–3569, Dec. 2017, doi: 10.11591/ijece.v7i6.pp3558-3569.
- [56] K. Rosenfeld and H. T. Sencar, “A study of the robustness of PRNU-based camera identification,” in *Media Forensics and Security*, Feb. 2009, vol. 7254., doi: 10.1117/12.814705.
- [57] M. Koopman, A. M. Rodriguez, and Z. Geradts, “Detection of deepfake video manipulation,” in *Proceedings of the 20th Irish Machine Vision and Image Processing conference*, 2018, pp. 133–136.
- [58] J. Pu, N. Mangaokar, B. Wang, C. K. Reddy, and B. Viswanath, “NoiseScope: detecting deepfake images in a blind setting,” in *Annual Computer Security Applications Conference*, Dec. 2020, pp. 913–927., doi: 10.1145/3427228.3427285.
- [59] R. A. Frick, S. Zmudzinski, and M. Steinebach, “Detecting ‘DeepFakes’ in H.264 video data using compression ghost artifacts,” *IS and T International Symposium on Electronic Imaging Science and Technology*, vol. 2020, no. 4, pp. 116–117, Jan. 2020, doi: 10.2352/ISSN.2470-1173.2020.4.MWSF-116.
- [60] X. Zhang, Z. H. Sun, S. Karaman, and S.-F. Chang, “Discovering image manipulation history by pairwise relation and forensics tools,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 1012–1023, Aug. 2020, doi: 10.1109/JSTSP.2020.2999827.
- [61] W. Zhang and C. Zhao, “Exposing face-swap images based on deep learning and ELA detection,” *The 5th International Electronic Conference on Entropy and Its Applications*. MDPI, Basel Switzerland, Nov. 2019., doi: 10.3390/ecea-5-06684.
- [62] M. A. S. Habeeba, A. Lijiya, and A. M. Chacko, “Detection of Deepfakes using visual artifacts and neural network classifier,” in *Innovations in Electrical and Electronic Engineering*, Springer, 2021, pp. 411–422., doi: 10.1007/978-981-15-4692-1\_31.

## BIOGRAPHIES OF AUTHORS






**Wildan Jameel Hadi**    has received her Bachelor's degree in computer science from Baghdad University in the year 2006. She has completed her Master's degree in Computer Science from the University of Technology in the Year 2008. She is currently pursuing her Ph.D. degree in computer science at Technology University, Iraq, and working in the Department of Computer Science, College of Science for women, University of Baghdad, Iraq. Her research interests include image processing, video analysis, deep learning, and face detection. She can be contacted at email: wildanjh\_comp@cs.w.uobaghdad.edu.iq.



**Suhad Malallah Kadhem**    has finished her Ph.D. in Computer Science from the Department of Computer Science at the Technology University. She has completed her bachelor's and master's degree in Computer Science from the University of Technology (UOT), Baghdad, Iraq in 1997. Suhad is a faculty member in the Computer Science Department at UOT since 1997, where she became the Head of the artificial intelligent branch at UOT in 2003. Her research interests focus on artificial intelligence, natural language processing (especially Arabic language processing), and computer security (especially steganography). She can be contacted at email: 110102@uotechnology.edu.iq.



**Ayad Rodhan Abbas**    has finished his Ph.D., Artificial Intelligent, Wuhan University, School of Computer Science, China, 2009, M.Sc., Computer Science, University of Technology, Computer Science Department, Iraq, 2005, B.S., Computer Science, University of Technology, Computer Science Department, Iraq, 2003, B.S., Chemical Engineering, University of Baghdad, Chemical Engineering Department, Iraq, 1999. His research interests focus on artificial intelligent, machine learning, natural language processing, deep learning, data mining, web mining, information retrieval, soft computing, e-learning, e-commerce, and recommended system. He can be contacted at email: 110010@uotechnology.edu.iq.