

## Analysis of the current state of deepfake techniques-creation and detection methods

Ashraf A. Abu-Ein<sup>1</sup>, Obaida M. Al-Hazaimeh<sup>2</sup>, Alaa M. Dawood<sup>3</sup>, Andraws I. Swidan<sup>3</sup>

<sup>1</sup>Department of Electrical Engineering, Al-Balqa Applied University, Irbid, Jordan

<sup>2</sup>Department of Computer Science and Information Technology, Al-Balqa Applied University, Irbid, Jordan

<sup>3</sup>Department of Computer Engineering, The University of Jordan, Amman, Jordan

### Article Info

#### Article history:

Received Jun 18, 2022

Revised Aug 26, 2022

Accepted Sep 9, 2022

#### Keywords:

Artificial intelligence

Celeb-DF

Deep learning

DeepFaceLab

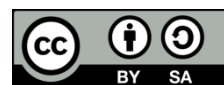
Deepfakes

Face manipulation

### ABSTRACT

Deep learning has effectively solved complicated challenges ranging from large data analytics to human level control and computer vision. However, deep learning has been used to produce software that threatens privacy, democracy, and national security. Deepfake is one of these new applications backed by deep learning. Fake images and movies created by Deepfake algorithms might be difficult for people to tell apart from real ones. This necessitates the development of tools that can automatically detect and evaluate the quality of digital visual media. This paper provides an overview of the algorithms and datasets used to build deepfakes, as well as the approaches presented to detect deepfakes to date. By reviewing the background of deepfakes methods, this paper provides a complete overview of deepfake approaches and promotes the creation of new and more robust strategies to deal with the increasingly complex deepfakes.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Obaida M. Al-Hazaimeh

Department of Computer Science and Information Technology, Al-Balqa Applied University

Irbid, Al-Huson, 21510, Jordan

E-mail: dr\_obaida@bau.edu.jo

## 1. INTRODUCTION

It's possible to generate videos that appear to show the target person doing or saying things that the source person does using techniques known as "Deepfakes" which derive their name from the words "deep learning" and "fake." The term "face-swap" is used to describe this type of deep fake. Deepfakes can also be lip-syncs or puppet-masters, depending on how the information is generated using artificial intelligence [1], [2]. This term is wide. A lip-sync deepfake refers to a video that has its lips movements synchronized to an audio recording. A puppet master deepfake includes footage of a target individual (i.e., puppet) animated following the facial emotions, eye and head movements of another person seated in front of a video camera [3], [4]. While traditional visual effects and computer graphics may be used to make certain deepfakes, deep learning models like GANs (i.e., "generative adversarial networks") and auto-encoders, which have been widely utilized in the sector of computer vision, are now the usual underlying mechanism for deepfake generation [5]. Figure 1 depicts a typical GAN model, which includes two neural networks: a generator and a discriminator. When analyzing a person's facial motions, these models help to synthesis images of another person with similar expressions and movements [6], [7].

To train models to produce videos and photo-realistic images, deepfake approaches often require a huge quantity of image and video data. Aside than generating realistic digital persons, deepfakes are used in visual effects, Snapchat filters, digital avatars, creating voices for those who have lost their voices, and updating movies without reshooting them [8]. As depicted in Figure 2, deepfake detection is divided into two

key categories: fake video detection techniques and fake image [5]. Discovering the truth in the digital world has become increasingly crucial. It is considerably more difficult when dealing with deepfakes, as they are predominantly utilized for harmful reasons and virtually anybody can construct deepfakes with existing deepfake tools today.

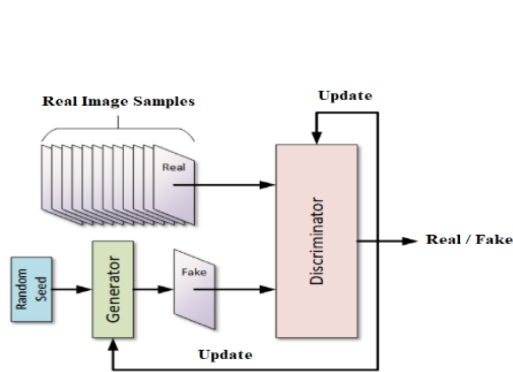


Figure 1. The architecture of GAN

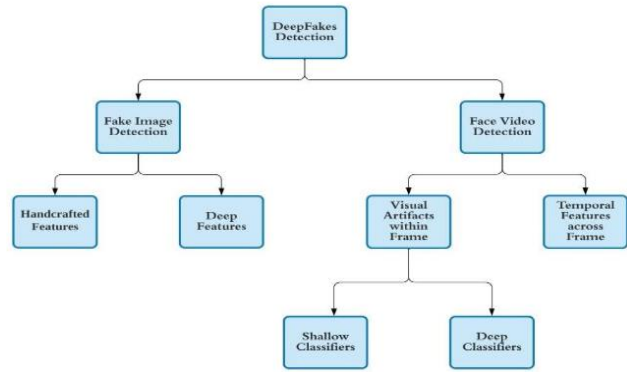


Figure 2. Categories of deepfake detection techniques

Face swapping between source and destination images utilizing autoencoder-decoder pairing structure requires two encoder-decoder pairs, with each pair trained independently on a different image set while sharing the encoder's parameters as shown in Figure 3. In other words, the encoder network is identical between the two pairs. Faces typically share features like eyes, noses, and mouth positions, making it easy for the common encoder to detect and learn the similarities between two sets of face images [7].

There have been various proposed approaches to identify deepfakes [9]. Most of them are based on deep learning, which has led to a struggle between malicious and beneficial applications of deep learning techniques. Defense advanced research projects agency (DARPA) established a research program in media forensics (called MediFor, or Material Foren) to speed up the development of technologies to detect fraudulent digital visual media as a response to the threat of deepfakes or face-swapping technology [10]. To make it clear, some examples face swaps from the dataset are shown in Figure 4. According to dimensions scholar, the quantity of deepfake publications has risen dramatically over the past few years, as seen in Figure 5 [11].

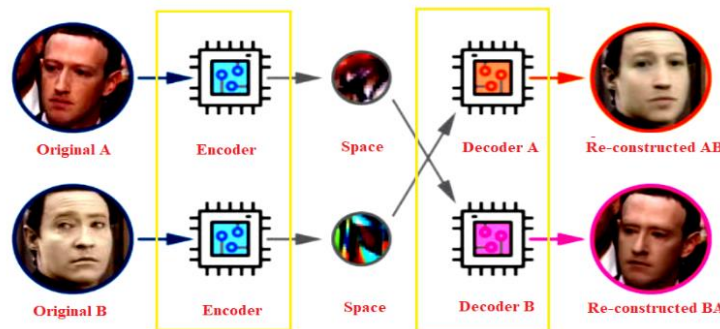


Figure 3. Two encoder-decoder pairs create a deepfake model

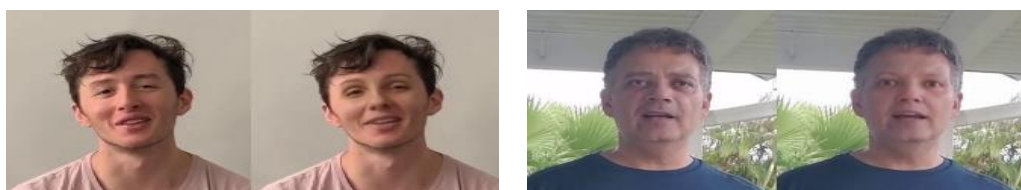


Figure 4. Face swapping example

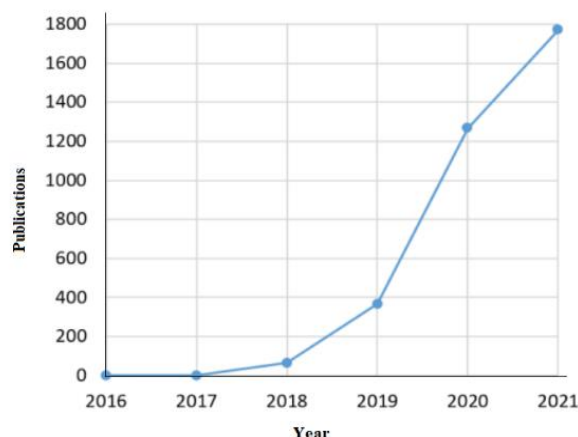


Figure 5. Quantity of deepfake publications in the period from (2016-2021)

## 2. DEEPFAKE CREATION AND DETECTION METHODS

Deepfake have gained popularity as a result of the high quality of their altered videos and the accessibility of their applications to people with varying levels of computer expertise, from experts to beginners. Deep learning techniques are mostly used to construct these applications [12]. Therefore, many computer vision researchers have taken up the deepfake detection problem. For example, Chang *et al.* [13] developed deepfake face image detection using an improved of the VGG network (i.e., "visual geometry group") based on augmentation and image noise. The image noise map is extended to weaken face features using an SRM filter layer (i.e., "style recalibration module"). Finally, the network is fed updated blurring images to train and detect fraudulent photos. Using the Celeb-DF dataset, NA-VGG out performed current false image detectors. Shad *et al.* [14] introduced a several ways to identify deepfake images and do comparison analyses were put in place. In this study, eight CNN structures are used to find deep fake images in a large data set. This is a comparison of how CNN (i.e., "Convolutional Neural Networks") can be used to distinguish between real and deep fake images.

A two-stream network was proposed by Zhou *et al.* [15] to detect face manipulation. On the other hand, GoogLeN was trained to detect artifact manipulation in the face categorization table, using a correction-based approach. For this new dataset, two online face-swap apps were used to modify 2010, resulting in 2010 modified photos. This data set was then utilized to assess the proposed two-stream network. In comparison to previous methods, the method's success is proved by its ability to learn both effects manipulation and residual hidden noise features.

Wodajo and Atnafu [16] created and developed a generalized deepfake video detection model using convolutional neural network (CNNs) and transformer. A convolutional vision transformer has two parts: a CNN and ViT (i.e., vision Transformer). ViT uses the attention approach to classify the acquired data, whereas CNN extracts the learnable features. The model trained on the DFDC dataset obtained 91.5% accuracy, a loss value of 0, and AUC of 0.91. In 2019, Zhang and Zhao [17] proposed a new deep learning-based method for identifying AI face photos from real-world facial images. Artificial intelligence (i.e., AI) facial recognition has been improved by using a new model based on deep learning and detection-level analysis. The proposed model has various advantages over current models, such as faster training period, fewer layers, and more efficiency. In Li and Lyu [3], a new method based on deep learning is explored for detecting false videos generated by artificial intelligence from actual videos. These fake videos are referred to deepfake videos. The existing deepfake algorithm can only generate images of restricted resolution, which then need to be adjusted further to match the faces to be substituted in the source video. This method is based on the observations that the current deepfake algorithm can only generate these images. This method has been assessed through the utilization of a number of different sets of deepfake videos that demonstrate its viability in application. Mo *et al.* [18] developed a CNN-based algorithm for detecting fake facial images and provide extensive experimental results showing that the proposed algorithm can accurately discriminate between false and real facial photos with an average accuracy of over 99.4%. Aside from that, while current GAN-based techniques can generate realistic-looking faces (or other visual objects and scenes), they will eventually generate statistical artifacts that prove fakes.

Hsu *et al.* [19] this study proposes a unique DeepFD (i.e., deep forgery discriminator) based on embedding the contrastive loss to detect fraudulent/manufactured images formed by modern GANs. Researchers could create a deep forgery discriminator to efficiently detect computer-generated photos (i.e.,

DeepFD). The proposed technology is the first to detect fraudulent photos. The contrastive loss may capture the combined discriminative properties of different GANs' fake images, which is the key contribution. It also improved classification performance and can visualize exaggerated aspects in fake photos. Experiments show that DeepFD effectively detected 94.7% of fake images made by advanced GANs. Kolagati *et al.* [20] constructed a deep hybrid neural network model to detect deep-fake videos. The facial landmarks detection is used to obtain information on a wide range of facial characteristics from the videos. In order to learn the difference between real and false videos, this data is assembled into a multilayer perceptron (i.e., MLP). Table 1 summarizes the most relevant research in the field of deepfake detection.

Table 1. The comparison of the relevant studies

Reference	Method	Year	Advantages	Performance evaluation Accuracy (%)
Chang <i>et al.</i> [13]	Convolutional neural network	2020	NA-VGG improved the detection of deepfake face images and the accuracy of this method. is much higher than several deepfake detection models.	85.70
Zhou <i>et al.</i> [15]	Neural networks	2017	It can detect tampering artifacts as well as hidden noise residual features. This method outperforms each stream by a large margin.	92.70
Wodajo and Atnafu [16]	Convolutional vision transformer	2021	This method's ability to detect deepfake, and quickly determine if the images are real or not.	91.50
Shad <i>et al.</i> [14]	Convolutional neural network	2021	Detect deepfake images with high accuracy. Accuracy, precision, F1-score, and area under the ROC curve were all highest for VGGFace.	99.00
Ismail <i>et al.</i> [21]	XGBoost	2021	The XGBoost algorithm uses more precise approximations to find the optimal tree model. It's designed to be adaptable and quick. It presents a fast and precise parallel tree boosting that solves many data science problems.	90.73
Ahmed <i>et al.</i> [22]	Rationale augmented convolutional neural network	2021	In a real-time environment, models that have better performance and are smaller in size will be more useful.	95.77
Rossler <i>et al.</i> [23]	Xception-Net	2019	Pre-training on ImageNet and larger network capacity allow XceptionNet to achieve compelling results on low quality images while maintaining reasonable performance.	95.73
Zhang and Zhao [17]	Deep learning and ELA Detection	2019	Less layers, less training time, more efficiency	97.00
Li and Lyu [3]	Transforms leave distinctive artifacts	2018	Simple image processing operations on an image can simulate artifacts directly.	99.90
Khalid and Woo [24]	One-class variational auto-encoder	2020	This method reconstructs real face images better than other methods. This shows that a one-class approach can effectively distinguish real (normal) images from anomalous (abnormal).	98.20
Liu <i>et al.</i> [25]	3D convolutional neural network	2021	The proposed network has fewer parameters than other networks. As well as reduces deployment consumption while maintaining detection performance.	99.83
Schroff <i>et al.</i> [26]	FaceNet-embedding	2015	A significant increase in the efficiency of representation.	99.63
Parkhi <i>et al.</i> [27]	Convolutional neural network	2015	This method provides the best performance and can be applied to a wide range of other tasks.	98.95
Güera and Delp [28]	Recurrent neural networks	2018	With only 2 seconds of video data, this algorithm can accurately predict whether a video has been manipulated.	97.10
Hsu <i>et al.</i> [19]	Generative adversarial network	2018	In terms of precision and recall rate, this approach outperforms other baseline approaches.	94.70
Marra <i>et al.</i> [29]	Generative adversarial network	2018	Deep networks, especially Xception-Net, are more robust and work well even when training-test mismatches.	89.00
Mo <i>et al.</i> [18]	Convolutional neural network	2018	A high visual quality fake face image can be distinguished from a real one using this method, which is effective in many situations.	99.40
Dang <i>et al.</i> [30]	Convolutional neural network	2018	The proposed system automatically extracts many abstract features, overcoming many challenges. and the model performed well on the dataset's imbalanced scenario.	98.00
Kolagati <i>at el.</i> [20]	Deep multilayer-Convolutional Neural Network	2022	The hybrid system is ideal for screening deepfake videos with high speed and low computational resources.	84.00
Khodabakhsh <i>et al.</i> [31]	Convolutional neural network	2018	Best results by a wide margin. Stable decision points are confirmed by lower error rates in conjunction with a lower EER error.	99.60

Using artificial intelligence techniques (i.e., cutting-edge), a developer created software that could replace one person's face with another. Deepfakes became popular in early 2018. A computer was fed a large number of still images of one individual and video footage of another in order for the procedure to function. With matching expressions such as lip-synch and other motions, the software then created a new film (i.e., fake) [12]. Table 2 provides an overview of deepfake's tools and features.

Table 2. List of the most popular deepfake tools

Reference	Tools	Features
[32]	DeepFaceLab	Multiple methods of face extraction are supported.
[10]	Faceswap-GAN	Auto-encoder architecture with adversarial and perceptual loss.
[10]	Faceswap	Using two pairs of encoder-decoder.
[33]	Few-Shot Face Translation	Latent embeddings Extraction for GAN processing using a model of face recognition (i.e., pre-trained).
[34]	DFaker	A loss function called DSSIM is utilized to reconstruct a face.
[34]	Deepfaketf	Similar toDFaker but using Tensorflow structure.
[35]	AvatarMe	Create 3D faces from arbitrary "wild" images
[36]	StyleRig	Annotations are not required for self-monitoring.
[37]	MarioNETte	Identity adaption does not necessitate a further fine-tuning process.
[17]	DiscoFaceGAN	Adopt 3D priors in adversarial.
[13]	StyleGAN	In the new architecture, high-level properties are automatically and unsupervised separated.
[12]	Face2Face	Face-to-face (i.e., Real time) reenactment of a monocular target video.
[36]	Neural Textures	Feature maps learned during scene capture and stored on top of 3D mesh proxies.
[38]	TransformableBottleneck Networks	Fine-grained 3D image modification.
[39]	Neural voice puppetry	Synthesis of audio-driven facial video.

### 3. EXPERIMENTAL EVALUATION

Generally, the performance of the algorithm (i.e., deepfake detection) is evaluated using the AUC scores (i.e., "Area under the curve") and ROC curve (i.e., "receiver operator characteristic"). The probability curve is known as the ROC, while the AUC represents the degree or amount of separation [40]-[47]. In other words, the ROC indicates how accurately the model predicts 0 and 1 classes as shown in Figure 6 [32]. The AUC represents the model's ability to identify between fake and real video [48]. Detection methods based on deepfake require training data and testing. As a result, the need for large-scale deepfake video datasets is growing. List of some current deepfake datasets are shown in Table 3. In addition, Figure 7 displays our evaluations of several existing deepfake datasets that vary in terms of release year, data sample size, and total number of distinct individuals [49]-[51]. To present the frame-level AUC scores for each mentioned dataset, six of the most effective state-of-the-art deepfake detection techniques that have been compared in this paper and the obtained results are listed in Table 4. Moreover, Figure 8 depicts the ROC curves for each technique in different large datasets such as FWA, MESO-4, MESOLNCEPTION-4, XCEPTION-C-23, XCEPTION-C-40, and DSP-FWA as shown respectively in Figures 8(a)-(f).



Figure 6. Probability of ROC curve

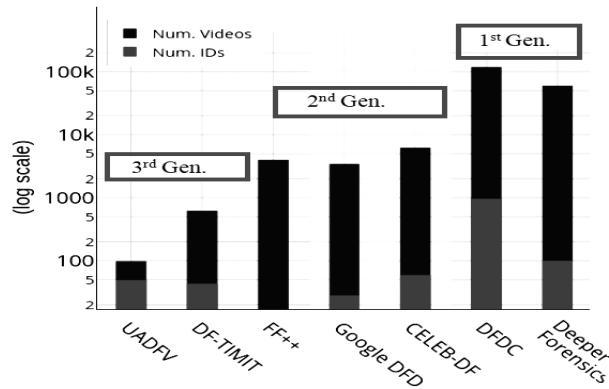


Figure 7. The fundamentals of several deepfake datasets

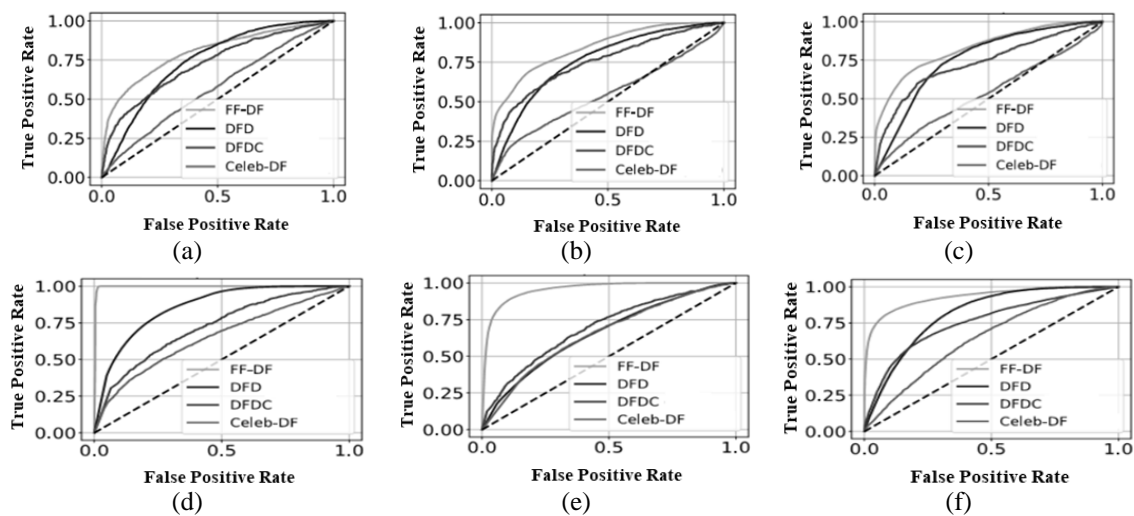


Figure 8. ROC curves (a) FWA, (b) MESO-4, (c) MESOLNCEPTION-4, (d) XCEPTION-C-23, (e) XCEPTION-C-40, and (f) DSP-FWA

Table 3. Quantitative analysis of existing deepfake datasets

Reference	Dataset	Real		Deepfake		Date of release	Description
		Frame	Video	Frame	Video		
[1]	DF-TIMIT-LQ DF-TIMIT-HQ	34.00k	320	34.00k	320	Dec. 2018	The Vid-TIMIT dataset was used to create 640 deepfake videos using Faceswap-GAN and the resulting Deepfake-TIMIT videos. DF-TIMIT-HQ and DF-TIMIT-LQ are equal-sized subsets of the videos.
[40]	DFDC	488.40k	1.131	1,783.30k	4,113	Oct. 2019	DFDC dataset consists of 4,113 deepfake videos based on 1,131 original videos of 66 persons of diverse genders, ages, and ethnicities.
[40]	FF-DF	509.90k	1.000	509.90k	1,000	Jan. 2019	The FaceForensics++ dataset contains 1,000 actual YouTube videos and 1,000 synthetic ones generated with Faceswap.
[41]	UADFV	17.30k	49	17.30k	49	Nov. 2018	UADFV has a total of 98 videos, 49 of which are real and 49 of which are deepfake. FakeAPP and the DNN model are used to generate the deepfake videos.
[41]	DFD	315.40k	363	2,242.7k	3,068	Sep. 2019	The deepfake detection dataset (Google/Jigsaw) consists of 3,068 deepfake videos created from 363 original videos.
[42]	Celeb-DF	225.40k	590	2,116.80k	5,639	Nov. 2019	The Celeb-DF dataset contains 5,639 deepfake videos and 590 real videos. The normal frame rate for videos is 30 frames per second, resulting in an average video length of approximately 13 seconds.

Table 4. AUC scores of the frame level

Reference	Technique	UADFV (%)	DF-TIMIT-LQ (%)	DF-TIMIT-LQ (%)	FF-DF (%)	DFD (%)	DFDC (%)	Celeb-DF (%)
[43]	DSP-FWA	97.70	99.90	99.70	93.00	81.10	75.50	64.60
[44]	MESOURCE-PTION-4	82.10	80.40	62.70	83.00	75.90	73.20	53.60
[45]	FWA	97.40	99.90	93.20	80.10	74.30	72.70	56.90
[46]	XCEPTION-C-23	91.20	95.90	94.40	99.70	85.90	72.20	65.30
[46]	XCEPTION-C-40	83.60	75.80	70.50	95.50	65.80	69.70	65.50
[44]	MESO-4	84.30	87.80	68.40	84.70	76.00	75.30	54.80

#### 4. CONCLUSION

Trust in media content has been eroded by deepfakes because seeing them is no longer equivalent to believing in them. In addition to causing distress and harm to the people they target, disinformation and hate speech propagated by them can also heighten political tensions, incite the population to violence or even war. Since deepfakes are becoming easier to create and spread on social media platforms, this is especially important now that the technology to do so is becoming more accessible. This survey provides an overview of deepfake creation and detection methods and discusses challenges, and trends. This study will help the artificial intelligence research community tackling deepfakes.

#### REFERENCES




- [1] Y. Li, X. Yang, P. Sun, H. Qi, and S. Lyu, "Celeb-df: A large-scale challenging dataset for deepfake forensics," *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020, pp. 3204-3213, doi: 10.1109/CVPR42600.2020.00327.
- [2] O. Al-hazaimeh, S. A. Alomari, J. Alsakran, and N. Alhindawi, "Cross correlation–new based technique for speaker recognition," *International Journal of Academic Research*, vol. 6, pp. 232-239, 2014, doi: 10.7813/2075-4124.2014/6-3/A.33.
- [3] Y. Li and S. Lyu, "Exposing deepfake videos by detecting face warping artifacts," 2018, [Online]. Available: <http://arxiv.org/abs/1811.00656>.
- [4] M. Al-Nawashi, O. M. Al-Hazaimeh, and M. Saraee, "A novel framework for intelligent surveillance system based on abnormal human activity detection in academic environments," *Neural Computing and Applications*, vol. 28, pp. 565-572, 2017, doi: 10.1007/s00521-016-2363-z.
- [5] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, "Generative adversarial networks: An overview," *IEEE Signal Processing Magazine*, vol. 35, no. 1, pp. 53-65, 2018, doi: 10.1109/MSP.2017.2765202.
- [6] T. Karras, S. Laine, and T. Aila, "A style-based generator architecture for generative adversarial networks," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2019, pp. 4396-4405, doi: 10.1109/CVPR.2019.00453.
- [7] O. M. Al-Hazaimeh and M. Al-Smadi, "Automated pedestrian recognition based on deep convolutional neural networks," *International Journal of Machine Learning and Computing*, vol. 9, no. 5, pp. 662-667, 2019, doi: 10.18178/ijmlc.2019.9.5.855.
- [8] L. A. Passos, D. Jodas, K. A. P. da Costa, L. A. S. Júnior, D. Colombo, and J. P. Papa, "A review of deep learning-based approaches for deepfake content detection," 2022, [Online]. Available: <http://arxiv.org/abs/2202.06095>.
- [9] H. M. Nguyen and R. Derakhshani, "Eyebrow recognition for identifying Deepfake videos," in *2020 international conference of the biometrics special interest group (BIOSIG)*, 2020, pp. 1-5.
- [10] S. Lyu, "Deepfake detection: Current challenges and next steps," *2020 IEEE international conference on multimedia & expo workshops (ICMEW)*, 2020, pp. 1-6, doi: 10.1109/ICMEW46912.2020.9105991.
- [11] T. T. Nguyen *et al.*, "Deep learning for deepfakes creation and detection: a survey," *Computer Vision and Image Understanding*, vol. 223, p. 103525, Oct. 2022, doi: 10.1016/j.cviu.2022.103525.
- [12] T. Zhang, L. Deng, L. Zhang, and X. Dang, "Deep learning in face synthesis: a survey on deepfakes," *2020 IEEE 3rd International Conference on Computer and Communication Engineering Technology (CCET)*, 2020, pp. 67-70, doi: 10.1109/CCET50901.2020.9213159.
- [13] X. Chang, J. Wu, T. Yang, and G. Feng, "Deepfake face image detection based on improved VGG convolutional neural network," in *2020 39th chinese control conference (CCC)*, 2020, pp. 7252-7256, doi: 10.23919/CCC50068.2020.9189596.
- [14] H. S. Shad, *et al.*, "Comparative analysis of deepfake image detection method using convolutional neural network," *Computational Intelligence and Neuroscience*, vol. 2021, p. 3111676, 2021, doi: 10.1155/2021/3111676.
- [15] P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, "Two-stream neural networks for tampered face detection," *2017 IEEE conference on computer vision and pattern recognition workshops (CVPRW)*, 2017, pp. 1831-1839, doi: 10.1109/CVPRW.2017.229.
- [16] D. Wodajo and S. Atnafu, "Deepfake video detection using convolutional vision transformer," 2021, [Online]. Available: <http://arxiv.org/abs/2102.11126>.
- [17] W. Zhang and C. Zhao, "Exposing face-swap images based on deep learning and ELA detection," *Proceedings*, vol. 46, no. 1, p. 29, 2020, doi: 10.3390/ecea-5-06684.
- [18] H. Mo, B. Chen, and W. Luo, "Fake faces identification via convolutional neural network," *Proceedings of the 6th ACM workshop on information hiding and multimedia security*, 2018, pp. 43-47, doi: 10.1145/3206004.3206009.
- [19] C.-C. Hsu, C.-Y. Lee, and Y.-X. Zhuang, "Learning to detect fake face images in the wild," *2018 International Symposium on Computer, Consumer and Control (IS3C)*, 2018, pp. 388-391, doi: 10.1109/IS3C.2018.00104.
- [20] S. Kolagati, T. Priyadarshini, and V. M. A. Rajam, "Exposing Deepfakes using a deep multilayer perceptron–convolutional neural network model," *International Journal of Information Management Data Insights*, vol. 2, no. 1, p. 10.1016/j.jjime.2021.100054, 2022, doi: 10.1016/j.jjime.2021.100054.
- [21] A. Ismail, M. Elpeltagy, M. S. Zaki, and K. Eldahshan, "A new deep learning-based methodology for video deepfake detection using XGBoost," *Sensors*, vol. 21, no. 16, p. 5413, 2021, doi: 10.3390/s21165413.






- [22] S. R. A. Ahmed and E. Sonuç, "Deepfake detection using rationale-augmented convolutional neural network," *Applied Nanoscience*, pp. 1-9, 2021, doi: 10.1007/s13204-021-02072-3.
- [23] A. Rossler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, "Faceforensics++: learning to detect manipulated facial images," *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 2019, pp. 1-11, doi: 10.1109/ICCV.2019.00009.
- [24] H. Khalid and S. S. Woo, "OC-FakeDect: classifying deepfakes using one-class variational autoencoder," *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops*, 2020, pp. 2794-2803, doi: 10.1109/CVPRW50498.2020.00336.
- [25] J. Liu, K. Zhu, W. Lu, X. Luo, and X. Zhao, "A lightweight 3D convolutional neural network for deepfake detection," *International Journal of Intelligent Systems*, vol. 36, no. 9, pp. 4990-5004, 2021, doi: 10.1002/int.22499.
- [26] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015, pp. 815-823, doi: 10.1109/CVPR.2015.7298682.
- [27] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Vedaldi A Zisserman A," *Proceedings of the British Machine Vision Conference 2015*, 2015, pp. 41.1-41.12, doi: 10.5244/C.29.41.
- [28] D. Güera and E. J. Delp, "Deepfake video detection using recurrent neural networks," *2018 15th IEEE international conference on advanced video and signal based surveillance (AVSS)*, 2018, pp. 1-6, doi: 10.1109/AVSS.2018.8639163.
- [29] F. Marra, D. Gragnaniello, D. Cozzolino, and L. Verdoliva, "Detection of gan-generated fake images over social networks," *2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, 2018, pp. 384-389, doi: 10.1109/MIPR.2018.00084.
- [30] L. M. Dang, S. I. Hassan, S. Im, J. Lee, S. Lee, and H. Moon, "Deep learning based computer generated face identification using convolutional neural network," *Applied Sciences*, vol. 8, no. 12, p. 2610, 2018, doi: 10.3390/app8122610.
- [31] A. Khodabakhsh, R. Ramachandra, K. Raja, P. Wasnik, and C. Busch, "Fake face detection methods: Can they be generalized?," in *2018 international conference of the biometrics special interest group (BIOSIG)*, 2018, pp. 1-6, doi: 10.23919/BIOSIG.2018.8553251.
- [32] I. Perov *et al.*, "DeepFaceLab: Integrated, flexible and extensible face-swapping framework," 2020, [Online]. Available: <http://arxiv.org/abs/2005.05535>.
- [33] N. Zhuang and C. Yang, "Few-shot knowledge transfer for fine-grained cartoon face generation," *2021 IEEE International Conference on Multimedia and Expo (ICME)*, 2021, pp. 1-6, doi: 10.1109/ICME51207.2021.9428473.
- [34] A. A. Maksutov, V. O. Morozov, A. A. Lavrenov, and A. S. Smirnov, "Methods of Deepfake detection based on machine learning," in *2020 IEEE conference of russian young researchers in electrical and electronic engineering (EIconRus)*, 2020, pp. 408-411, doi: 10.1109/EIconRus49466.2020.9039057.
- [35] A. Hilton, "Computer vision for human modelling and analysis," *Machine Vision and Applications*, vol. 14, pp. 206-209, 2003, doi: 10.1007/s00138-003-0123-4.
- [36] A. Tewari *et al.*, "Stylerig: Rigging stylegan for 3d control over portrait images," *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020, pp. 6141-6150, doi: 10.1109/CVPR42600.2020.00618.
- [37] D. Smirnov, M. Gharbi, M. Fisher, V. Guizilini, A. A. Efros, and J. Solomon, "MarioNette: self-supervised sprite learning," 2021, [Online]. Available: <http://arxiv.org/abs/2104.14553>.
- [38] J. Ren, M. Chai, O. J. Woodford, K. Olszewski, and S. Tulyakov, "Flow guided transformable bottleneck networks for motion retargeting," *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021, pp. 10790-10800, doi: 10.1109/CVPR46437.2021.01065.
- [39] M. P. Aylett, D. A. Braude, C. J. Pidcock, and B. Potard, "Voice puppetry: exploring dramatic performance to develop speech synthesis," *10th ISCA Workshop on Speech Synthesis (SSW 10)*, 2019, pp. 117-120, doi: 10.21437/SSW.2019-21.
- [40] B. Dolhansky, R. Howes, B. Pflaum, N. Baram, and C. C. Ferrer, "The deepfake detection challenge (DFDC) preview dataset," 2019, [Online]. Available: <http://arxiv.org/abs/1910.08854>.
- [41] D. Feng, X. Lu, and X. Lin, "Deep detection for face manipulation," *International Conference on Neural Information Processing*, 2020, pp. 316-323, doi: 10.1007/978-3-030-63823-8\_37.
- [42] N. Gharaibeh, O. M. Al-hazaimeh, A. Abu-Ein, and K. M. Nahar, "A hybrid svm naïve-bayes classifier for bright lesions recognition in eye fundus images," *Int J Electr Eng Inform*, vol. 13, pp. 530-545, 2021, doi: 10.15676/ijeei.2021.13.3.2.
- [43] 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, doi: 10.1109/CVPR42600.2020.00327.
- [44] D. Afchar, V. Nozick, J. Yamagishi and I. Echizen, "MesoNet: a compact facial video forgery detection network," *IEEE International Workshop on Information Forensics and Security (WIFS)*, 2018, pp. 1-7, doi: 10.1109/WIFS.2018.8630761.
- [45] Y. Li and S. Lyu, "Exposing deepfake videos by detecting face warping artifacts," 2018, [Online]. Available: <http://arxiv.org/abs/1811.00656>.
- [46] A. Rossler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, "Faceforensics++: learning to detect manipulated facial images," *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 2019, pp. 1-11, doi: 10.1109/ICCV.2019.00009.
- [47] K. Nahar, O. M. Al-Hazaimeh, A. Abu-Ein, and N. Gharaibeh, "Phonocardiogram classification based on machine learning with multiple sound features," *Journal of Computer Science*, vol. 16, no. 11, pp. 1648-1656, 2020, doi: 10.3844/jcssp.2020.1648.1656.
- [48] A. Abdulreda and A. Obaid, "A landscape view of deepfake techniques and detection methods," *International Journal of Nonlinear Analysis and Applications*, vol. 13, no. 1, pp. 745-755, 2022, doi: 10.22075/IJNAA.2022.5580.
- [49] F. Lugstein, S. Baier, G. Bachinger, and A. Uhl, "PRNU-based deepfake detection," *Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security*, 2021, pp. 7-12, doi: 10.1145/3437880.3460400.
- [50] L. A. Passos, D. Jodas, K. A. P. da Costa, L. A. S. Júnior, D. Colombo, and J. P. Papa, "A review of deep learning-based approaches for deepfake content detection," 2022, [Online]. Available: <http://arxiv.org/abs/2202.06095>.
- [51] O. M. Al-Hazaimeh, M. Al-Nawashi, and M. Saraee, "Geometrical-based approach for robust human image detection," *Multimedia Tools and Applications*, vol. 78, pp. 7029-7053, 2019, doi: 10.1007/s11042-018-6401-y.






**BIOGRAPHIES OF AUTHORS**

**Ashraf A. Abu-Ein**    is an Associate Professor in the Department of Electrical Engineering. He has completed his Ph.D at National Technical University of Ukraine, Computer Engineering. “Computers, Computing Systems and Networks”, 2007. Now, he is a lecturer at Al-Balqa Applied University-AI-huson University College, Jordan. He can be contacted at email: ashraf.abuain@bau.edu.jo.






**Obaida M. Al-Hazaimeh**    earned a BSc in Computer Science from Jordan's Applied Science University in 2004 and an MSc in Computer Science from Malaysia's University Science Malaysia in 2006. In 2010, he earned a Ph.D in Network Security (Cryptography) from Malaysia. He is a Full professor at Al-Balqa Applied University's department of computer science and information technology. Cryptology, image processing, machine learning, and chaos theory are among his primary research interests. He has published around 45 papers in international refereed publications as an author or co-author. He can be contacted at email: dr\_obaida@bau.edu.jo.



**Alaa M. Dawood**    received a BSc in Computer engineering techniques from Al-Mamoon University College in 2015 in Baghdad and a Master student in Department of Computer Engineering from University of Jordan. She can be contacted at email: ala8181789@ju.edu.jo.



**Andraws I. Swidan**    he is a Full professor at University of Jordan-Electrical and Computer Engineering Department. He has authored and co-authored of various papers in international peer-reviewed journals. He can be contacted at email: sweidan@ju.edu.jo.