

## A robust facemask forgery detection system in video

Firas Husham Almkhtar

Information Technology Department, Catholic University in Erbil – KRG, Iraq

### ABSTRACT

An in-depth fake video uses an Artificial Intelligent (AI), AI programming, and a Personal computer (PC) mix to create a deep fake video of the action. Deep-faking can also be used to represent images and sounds. We provide insights into our reviews in this document. We're showing our dataset to start. At this point, we present the subtleties and reproductively of exploratory settings to evaluate the discovered effects finally. It is no surprise to find deep fake videos, which only monitor a tiny section of the video (e.g., the target face appears quickly on the video; hence the time is limited). We remove our system's fixed duration's persistent effects as each video contributes to the preparation, approval, and testing sections to reflect this. The edge groups are isolated from each video successively (without outline skips). The entire pipeline is ready to be finished when the approval stage is ten years old. Convolutional Neural Network (CNN) was the best and most reliable of the classification systems. Fake videos typically use low-quality pictures to mask faults or insist that the general public regard camera defects as unexplainable phenomena. This is a common trope with Unidentified Flying Object (UFO) videos: ghostly orbs are lenses; snakes are compression artifacts on one's face. In this study, we have implemented a sophisticated, knowledgeable method to recognize false images. Our test results using various monitored videos have shown that we can reliably predict whether videos are monitored through with simple co-evolutionary Long Short-Term Memory (LSTM) structure.

**Keywords:** Fake video, Artificial Intelligent (AI), AI programming, Deep-faking, Images, Convolutional Neural Network (CNN)

### Corresponding Author:

Firas Husham Almkhtar  
Information Technology Department  
Catholic University in Erbil – KRG, Iraq  
Email: [f.almukhtar@cue.edu.krd](mailto:f.almukhtar@cue.edu.krd)

### 1. Introduction

The problem of Presentation Attack Detection (PAD) has plagued facial recognition since biometric technologies have been applied in many mobile and control systems. Mobile payments and phone unlocking have been made possible by Apple's iPhone X face ID. Kuar researchers have devised a mask that can deceive the Face ID system in Vietnam, according to Kaur and Jindal [1]. A 3D face mask PAD technique that is both effective and trustworthy must be developed in light of the current pressing need for safety [2]. The mask must be complete without occlusion, while traditional results of segmentation exclude the occluded area. Available facial masks may have many potential and exciting applications, including face detection and identification, identification of emotion and speech, social robot interactions, etc. [3],[4]. To our knowledge, this is the first analysis of a video sequence face mask with a more in-depth learning model that was trained from one end to the other [5]. The role of counterfeit classification is to recognize forged images. It is cast based on manipulated images as a binary classification issue. Since there are no particular approaches for Face2Face manipulation in the current documentation, we have opted to research methods for detecting overall deception, computer-generated images, and facial deception [6]. We had an advanced deep network as well [7]. The method consists of 10 frames, each of 704 forged videos and 704 new videos, which have been trained in the same set of data. The test set consists of 10 frames, each from 150 [pristine] and 150 [fake] frames [8],[9]. For each frame, we use the mask given by Face2Face for all images based on the face. On request, to the network input size; otherwise, a 128x128 pixel clip centered on the front is extracted from the input size. For all baselines, quality



parameters for hundreds uncompressed and compression are calculated in a range of distribution channels, including popular social networks [4]. Two hundred sixty-four compressed data with parameters of quantification equivalent to 23 light compression and 40 strong compressions [10]. CNN is also a standard, widely used algorithm for profound learning. It was thoroughly integrated into various applications such as NLP (Natural Language Processing), speech recognition, and computer vision [11]. The development of the animal and human brains influences the neurons, similarly to conventional neural networks. In a cat brain with a complex cell-sequence, the visual cortex is precisely simulated. [12], published. CNN provides three significant advantages: criteria of sharing sparsely interacted, etc. Instead of traditional completely connected networks, the two-dimensional input data structure (for example, the imaging) is thoroughly utilized by local connectors and mutual network weights. These cells are more susceptible than the whole scene to small parts of the stage. In other words, the cells act as local filters over the input and eliminate local interrelationships [13]. Video and pictures are usually useful to people. Many systems and applications have recently started to automate their tasks with video analytical algorithms [14]. These systems provide video monitoring, separate vehicles, and small mobiles [15]. For example, a video monitoring system automates a video analysis before a sudden incident occurs without alerting the human guard: Independent aircraft monitors or tracks targets based on the video analysis results. Amateur mobile telephones automatically tag a picture and mark the current location based on an area analysis [16]. The video is processed first on the sensor, and the results which be transmitted to the server. Secondly, the video streams will be sent to the server and stored on the server. This investigation aims to review current research on face detection in videos [17],[18].

## 2. Method

A Deep-fake video utilizes a blend of AI, AI programming, and a PC to make a deep-fake video of the action. Deep-faking can likewise be used to portray sound and photographs. Later on, deep-fake videos will become generally well known to influence legislative issues and increment cybercrime. In the realm of the governmental problems, it's relied upon to make disarray for competitors and authorities with videos of things they didn't state to diminish their believability. Deep-fake videos can prompt genuine risks surprisingly fast and encourage various perils if not cautious [19]. In the past decade, facial detection has progressed considerably, mainly because of progress on deep learning and CNNs. As a result, CNN-based facial identification systems are now capable of detecting faces with complex traits and variability across poses, scales, and lighting conditions, even in the presence of other nuisances such as low-quality data. Research into face detection for various occlusions has been done, but there has been little research into face detection for masked faces. The model was chosen for our studies because of its competitive performance and that the models concerned are publicly available. There are also face mask detection frameworks specifically created for the detection problem being addressed [20]. CNN has a major role in computer vision-related pattern detection tasks based on its superior space extraction and lower computational costs. CNN uses convolution kernels to extract higher level properties to complement the original images or feature maps. An opening question remains, however, how better neural network architectures can be developed. The proposed network allows the network to learn the best combinations of kernel systems. The Residual Network (ResNet) [6] can learn ID cards of the last level and forms much deeper neural networks. [4], as object detectors are usually used in mobile devices or embedded devices with limited computer resources, mobile networks are suggested [21]. It uses a deep convolution in order to extract functions and canal convolutions in order to adjust the number of canals, so that the cost of calculations of MobileNet is considerably lower than for standard networks. There are two ways to detect a profound video. The first is to see an image as real or profound and set the threshold, given that the video, if the number of fake frames  $>$  thresholds, is profound; otherwise, the video is not profound. Due to the substantial decrease in edge information after video compression, most image techniques were unused for images. Moreover, videos have transient qualities modified between frames, and the identification of deep-fault images becomes difficult for the design system. This subsection focuses on profound video recognition methods and orders them in two sessions: approaches that use transitional highlights and analyzed visual objects in frameworks. Deep-fake videos have been shown to include intra-frame incoherence's and temporal differences between frames. We use a time-conscious pipeline method using CNN and long-term memory (LTM) to detect deep fake videos [22-26]. To verify if face masks are being used correctly, all the faces that were recognized were grouped into one class. First-class faces are those with a mask that properly covers the nose, lips, and chin. No masks or masks incorrectly positioned constitute the second class of faces. Using this configuration, we can trim and resize the face regions of the input images [21].

### 3. Experiments

We used the Stochastic Gradient Descent (SGD) as an algorithm of optimization in experiments  $\alpha = 10^{-3}$ ,  $\beta$  momentum = 0.9 and 250 epochs. The database has been separated into a train, validation and test set. The size of the input image is 840 to 840 and batch size 2 for the ResNet backbone; the size of the input image is 640 to 640 to 32 for the MobileNet backbone [27,28].

#### 3.1. Setting dataset and parameters

First, we have used an abnormal portion to build three disjoint sets, used separately for planning, approval, and testing. We make a rational division, i.e., divided first into the 300 in-depth fake videos, and then we re-start the loop for the 300 unregulated videos. Ensures that every last collection contains exactly half of each class videos, allowing us to report our results on precision without considering inclinations due to the recurrence of each class's presence or the need for regularizing conditions during preparation [23]. Concerning the preprocessing of details for video classes, we do:

- I was subtracting from each channel average. Each case needs to be resized.
- Sub-grouping of length exams N regulating information arrangement length –  $N = 20, 40, 80$  cases. The information causes the number of edges per video to be critical for an exact discovery.
- Adam is set to streamline to begin preparing the complete model with a learning speed of  $1e^{-5}$  and a rot of  $1e^{-6}$ .

### 4. Results and discussion

#### 4.1. The results

It's no surprise to discover deep fake videos that control only a small part of the video (e.g., the objective face appears fast on the video, so the control is limited in time). To reflect this, we exclude persistent effects of fixed edge length as our system's contribution for each video in the planning, approval, and testing sections. Edge groups are successively separated from each video (without outline skips). The entire pipeline is ready for completion when we hit a 10-year misfortune stage of approval. Among the classification schemes, CNN was best and precise. Some screenshots are attached below:

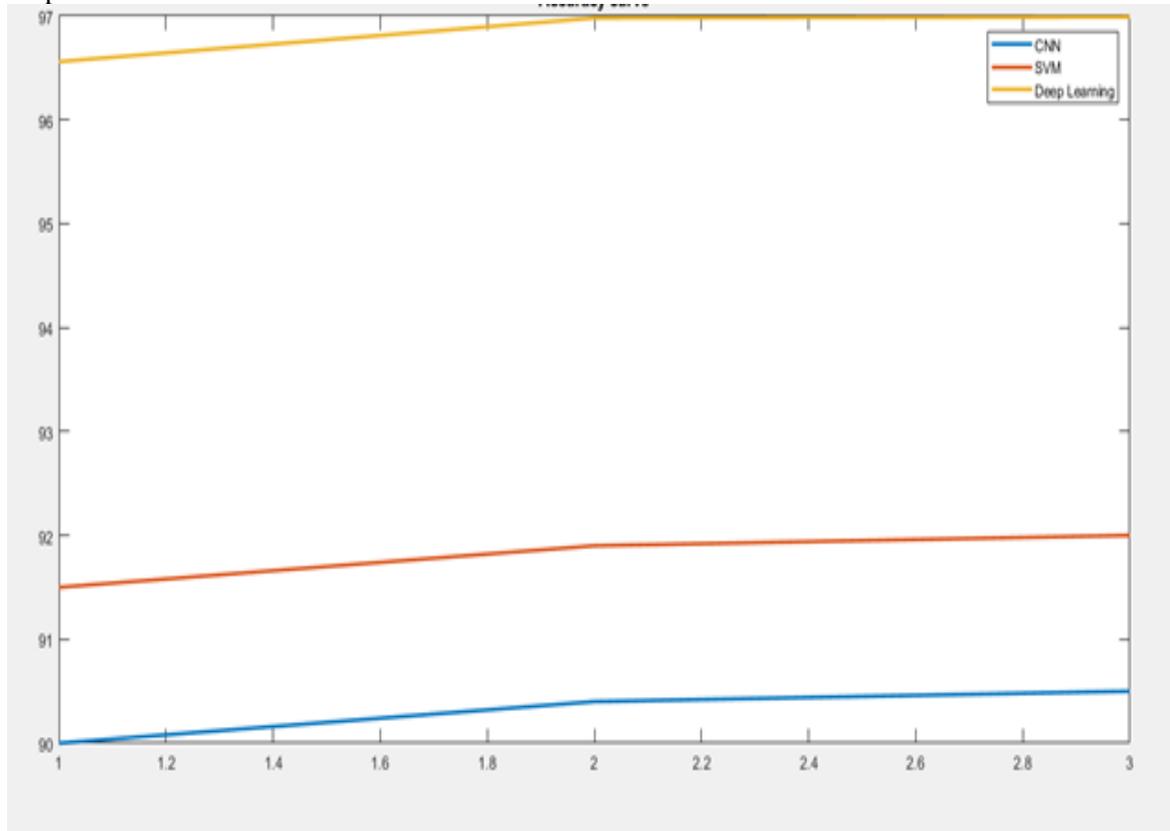


Figure 1. The final result and comparison of the classifier



Figure 2. Detection of the image as Non-Fake Image



Figure 3. Detection of the image as Fake Image

#### 4.2. The discussion

This study showed a comparison of two images; a fake image and a real picture. For the first time, people have minimal ability to detect manipulated real-world photographs. Our findings warrant that people often tamper within their everyday lives. We also found no strong evidence that factors like a photographic interest or beliefs

on the extent of image manipulation in society are related to an enhanced ability to detect or locate the manipulation. The final result and classifier comparison are illustrated in Figure 1. Non-expert users often adopt the default values of the classifiers and provide a logical starting point for specialist researchers. We have used the following parameters on the aforementioned algorithm to create the artificial datasets to provide comprehensive comparison between classifier. The aim is to avoid other classifier from reaching too extreme values by fixing the accuracy rate of a classifier. A real image and a fake image are different, but they look the same (Figure 2 and 3). The main difference between real and fake images is their manner of producing them. When rays converge, there is a real image, while a fake picture appears when rays seem only to differentiate. The comparisons of fake and real images were shown in this article in Figures 2 and 3. The light source and display must be placed on the same level to obtain a real image. A converging lens or a concave mirror is used to obtain the image. The image size depends on how the object is positioned. In contrast, the fake image is a right picture that can be obtained where the rays appear to differ but do not actually converge. According to Bappy [29], removing elements is generally much more comfortable than adding them, and you should keep this in mind when looking at the videos. Fake videos often use low-quality images to conceal flaws or demand that audiences perceive common camera flaws as unexplainable phenomena. "That's a common trope with UFO videos: ghostly orbs are lens flares, reptile disguises are compression objects on one's face. Our analysis has made three significant improvements in contrast with previous studies [30]. Firstly, our architecture has acknowledged that image consumption and appraisal on the Internet are often contextual rather than vacuum. Therefore, we give brief textual information on an image made, similar to how images are typically displayed and viewed online. Secondly, we have specifically manipulated and checked whether an intermediary's role and trustworthiness affect image credibility assessment, taking online knowledge exchanged and exchanged by different sources. Third, we have adopted a credibility measure (6 objects, 7-point) that is more complex than a binary yes / no choice, used in Bappy [29]. Our scale is more accurate and efficient than a binary metric, which is likely to produce false-positive and negative results. Our research's most important finding is that the viewers' skills and expertise impact their credibility assessments. The better people's awareness and experience with the Internet, digital photography, and digital media channels, the better they can determine the picture's credibility. Our findings stated to minimize the possible damage caused by false photos online; the best approach is to invest in education to improve consumer digital media literacy [9]. Meanwhile, the attitude to the problem also has a significant impact. In several related research [31], this illustrates the confirmatory bias that people are more likely to consider a picture as accurate if it aligns with their earlier beliefs. This result may explain why fake news so quickly spreads in social media environments. People's faith in media content is being eroded by deep fakes, making it impossible to distinguish between what one sees and what one believes. Could make individuals who are being targeted feel the terrible effects of their attention; raise the level of disinformation and ridicule speech; or worse, incite political strife or war. Since deep-fakes are becoming more accessible, and web-based media platforms can quickly propagate the unnatural substance, today's influence is fundamental. Deep-fakes are not always appropriate for large crowds because they can have negative effects. Those who create deep fakes for malignant purposes must communicate them to their intended victims without using internet media [32]. According to Kaur and Jindal [29], this strategy can be utilized by insight agencies to influence the decisions of prominent individuals, such as parliamentarians, resulting in public and global security threats. Deep-fake location calculations have been the focus of the study network, and several outcomes have been taken into account. This paper has checked on the cutting-edge strategies and a rundown of typical methodologies. It is observable that a fight between the individuals who utilize progressed AI to make deep- fakes with the individuals who attempt to recognize deep-fakes is developing [33]. As the quality of deep-fakes grows, so should the display of identifying methods. To put it another way, the motive is that what AI has broken can also be mended by AI. As a new field, location techniques are still in their infancy, and various approaches have been developed and tested, all of which use segmented informational indexes. It is good to keep a new set of deep-fake informative benchmarks to ensure that recognition techniques are always improving. Location models that rely on deep-fake realization, which necessitates a large preparation set, will benefit from the improvement because it will stimulate the preparation cycle. Alternatively, existing discovery methods often focus on the drawbacks of deep-fake age pipelines, for example, uncovering deficiencies of the competitors to attack them. This kind of data and knowledge is rarely available in combat situations, as attackers are typically trying to keep such deep-fake production advancements hidden from view. Future research must focus on delivering more robust, flexible, and generalizable solutions for location strategy advancement in the state. Another examination course is to incorporate recognition strategies into conveyance stages, for example, online media to expand its viability in managing the overall effect of deep-fakes [34]. The screening or separating component utilizing

effective identification techniques can be actualized on these stages to facilitate the deep-fakes location. Legitimate necessities can be made for tech organizations who own these stages to eliminate deep-fakes rapidly to lessen its effects [35]. Moreover, watermarking instruments can likewise be incorporated into gadgets that individuals use to make advanced substance to make unchanging metadata for putting away inventiveness subtleties, for example, time and area of media substance just as their untampered attachment. This coordination is hard to actualize; however, an answer could be utilizing the problematic block chain innovation. The block chain has been used adequately in numerous territories, and there are not many examinations so far tending to the deep-fake location issues dependent on this innovation. As it can make a chain of attractive unchangeable squares of metadata, it is an extraordinary device for computerized provenance arrangement. The joining of block chain innovations to this issue has shown specific outcomes [16]; however, this exploration course is long from development. However, while it is critical to employ discovery tools to identify deep fakes, it is even more critical to understand the true motivations of those who distribute them. For example, who delivered the deep-fake and what they said about it affects the client's perception of the result [30]. Due to the rising photo-realism of deep-fakes, it is predicted that identification programs will fall behind deep-fake creation innovations. Consequently, it is worthwhile to investigate social settings that are deep-faked to assist customers in making such judgments [10]. In police examinations and equity trials, videos and images have been widely used as confirmations. Experts in computerized media criminology who have a background in PC or law enforcement and extensive experience in obtaining, looking at, and analyzing advanced data may be able to submit them as evidence in an official courtroom [17]. Artificial intelligence (AI) progress and AI advances may have altered this digital substance. Because even experts cannot identify the controlled substance, the experts' conclusions may not be sufficient to support these findings. This viewpoint needs to consider in courts these days when pictures and videos are utilized as confirmations to convict culprits in light of the presence of a broad scope of advanced control strategies [36]. The computerized media legal sciences result accordingly should end up being legitimate and dependable before they can be utilized in courts. The data requires cautious documentation for each progression of the crime scene investigation cycle and how the outcomes are reached. AI and AI calculations can help the assurance of computerized media's legitimacy and have acquired exact and dependable results; however, the majority of these calculations are unexplainable. The data makes a gigantic obstacle for AI utilization in crime scene investigation issues because not just the legal sciences specialists regularly don't have skill in PC calculations. However, the PC experts likewise can't clarify the outcomes appropriately as the more significant part of these calculations is discovery models. The discovery is essential as the latest models with the most exact results depend on deep-fake learning techniques comprising numerous neural organization boundaries. Reasonable AI in PC vision in this way is an examination heading that is expected to advance and use the advances and focal points of AI and AI in computerized media legal sciences [37-45].

## **5. Conclusion and future suggestions**

In this article, we have implemented a sophisticated aware system to identify fake images. Our test results using a vast array of monitored videos have shown that using a fundamental coevolutionary LSTM structure, we can reliably predict whether videos have been scanned with as many as 2 seconds of video knowledge. We agree that our work provides a pioneering first line of defense to detect falsified media made using the devices seen in the paper. We demonstrate how our architecture can produce profound results using a simple pipeline design. In future work, we shall discuss how to construct our system's strength against monitored videos using concealed methods during planning. Given the standard video analysis algorithms' heterosporous and empirical existence, all the algorithms cannot generalize the findings. However, we assume that non-trivial and useful video analysis algorithms can be grouped into a small number of groups that respond similarly to different video quality reductions. Algorithms are often focused on observational data or training; their actions may be hard to formalize completely. Therefore, experiments with more examples of algorithms would support the hypothesis that video analysis algorithms need fewer quality videos than humans. In general, the paper results demonstrate that video analysis controlling algorithms is inefficient and inefficient in the same way a human video observer is ineffective video analytics, which can and should be built as resource-efficient algorithms. Computer vision video encoding algorithms should be developed because computer views vary widely in the required video quality from human vision. Note that CNN multi-task can be pre-trained on ImageNet data rather than using the network attribute information parameters. However, we find that the multi-task CNN converges much quicker, offering the retrained model based on facial attributes. In particular, 45,000 iterations during the face detection process are needed for the retrained network attribute to converge, compared with more than 200,000 for the

network belonging to the image network's visible size. We believe that far fewer efforts are necessary to translate the characteristics acquired from the classification of face attributes into facial detection. It is shown that the CNN face detector beats all other standalone methods. However, a group that combines CNN with different types of face detectors illustrates its self-sufficient efficiency. The number of facial sensors in a series increases the number of false positives. Still, this figure reduces to acceptable quantities with the current filter cascade, as shown in the experiments described in this article. In real-time, the proposed multi-face monitoring model takes into account multi-color video monitoring. Faces are detected by color image information. Facial recognition is not dependent on the multidimensional translation of the image. The proposed approach is therefore low-computational. The underlying facial sensing algorithm uses image color information. Thus, it is impossible to detect the face of gray ideas. The skins detected are filtered by extracting minimal skin components from noises. The model cannot, therefore, see very tiny camera images. The model will, however, differentiate between faces and pictures of a low-resolution film or frames. The model is also related to the image faces. The aim is to register images if the traced faces are for further use. This model's advantage is that it can recognize fluid images and side images, as in other traditional models. The only drawback is that glasses cannot distinguish the eyes. The weighting factor will increase the machine's accuracy with the short approximate neighbor search library (FLANN which stands for Functional Link Artificial Neural Network). The architecture has been applied and tested in real-time with YouTube and Extended Yale B databases and metrics. Experimental studies indicate that it takes less time to classify your face and achieve a particular result. A more extensive database can future check the suggested solution, and clustering algorithms can reduce recognition time. The Face Recognition system's accuracy can be improved by profound learning methods such as the Convolution Neural Network. Thus, it can be extended to allow people to recognize the person from the CCTV (Closed Circuit Television) cameras through video capture. It is also ideal for domestic security systems.

### Declaration of competing interest

The authors declare that they have no any known financial or non-financial competing interests in any material discussed in this paper.

### Funding information

No funding was received from any financial organization to conduct this research

### References

- [1] H. Kaur and N. Jindal, "Deep Convolutional Neural Network for Graphics Forgery Detection in Video," *Wirel. Pers. Commun.* 2020 1123, vol. 112, no. 3, pp. 1763–1781, Jan. 2020, doi: 10.1007/S11277-020-07126-3.
- [2] Y. Sun, D. Liang, X. Wang, and X. Tang, "DeepID3: Face Recognition with Very Deep Neural Networks," Feb. 2015, doi: 10.48550/arxiv.1502.00873.
- [3] B. Yang, J. Yan, Z. Lei, and S. Z. Li, "Fine-grained evaluation on face detection in the wild," *2015 11th IEEE Int. Conf. Work. Autom. Face Gesture Recognition, FG 2015*, Jul. 2015, doi: 10.1109/FG.2015.7163158.
- [4] B. Zhang *et al.*, "DeepFireNet: A real-time video fire detection method based on multi-feature fusion," *Math. Biosci. Eng.* 2020 67804, vol. 17, no. 6, pp. 7804–7818, 2020, doi: 10.3934/MBE.2020397.
- [5] Y. Tian *et al.*, "Feature fusion-based preprocessing for steel plate surface defect recognition," *Math. Biosci. Eng.* 2020 55672, vol. 17, no. 5, pp. 5672–5685, Aug. 2020, doi: 10.3934/MBE.2020305.
- [6] B. Batagelj, P. Peer, V. Štruc, and S. Dobrišek, "How to Correctly Detect Face-Masks for COVID-19 from Visual Information?," *Appl. Sci.* 2021, Vol. 11, Page 2070, vol. 11, no. 5, p. 2070, Feb. 2021, doi: 10.3390/APP11052070.
- [7] B. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," *IH MMSec 2016 - Proc. 2016 ACM Inf. Hiding Multimed. Secur. Work.*, pp. 5–10, 2016, doi: 10.1145/2909827.2930786.
- [8] T. Wen, H. Wu, Y. Du, and C. Huang, "Faster R-CNN with improved anchor box for cell recognition," *Math. Biosci. Eng.*, vol. 17, no. 6, pp. 7772–7786, Nov. 2020, doi: 10.3934/MBE.2020395.

- [9] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks," *IEEE Signal Process. Lett.*, vol. 23, no. 10, pp. 1499–1503, Apr. 2016, doi: 10.1109/LSP.2016.2603342.
- [10] Z. Wang *et al.*, "Masked Face Recognition Dataset and Application," Mar. 2020, doi: 10.48550/arxiv.2003.09093.
- [11] A. Khamparia, D. Gupta, N. G. Nguyen, A. Khanna, B. Pandey, and P. Tiwari, "Sound classification using convolutional neural network and tensor deep stacking network," *IEEE Access*, vol. 7, pp. 7717–7727, 2019, doi: 10.1109/ACCESS.2018.2888882.
- [12] L. Xiang *et al.*, "A convolutional neural network-based linguistic steganalysis for synonym substitution steganography," *Math. Biosci. Eng. 2020 21041*, vol. 17, no. 2, pp. 1041–1058, 2020, doi: 10.3934/MBE.2020055.
- [13] V. Badrinarayanan, A. Kendall, and R. Cipolla, "SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 12, pp. 2481–2495, Dec. 2017, doi: 10.1109/TPAMI.2016.2644615.
- [14] Rao, T.S., Devi, S.A., and Ram, P.M., "A Novel Approach to Detect Face Mask to Control Covid Using Deep Learning," *European Journal of Molecular and Clinical Medicine*, vol. 7, no. 5, pp. 658–668, 2020.
- [15] B. S. A. Alhayani *et al.*, "Optimized video internet of things using elliptic curve cryptography based encryption and decryption," *Comput. Electr. Eng.*, vol. 101, p. 108022, Jul. 2022, doi: 10.1016/J.COMPELECENG.2022.108022.
- [16] C. Szegedy *et al.*, "Going Deeper with Convolutions," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 07-12-June-2015, pp. 1–9, Sep. 2014, doi: 10.48550/arxiv.1409.4842.
- [17] L. S. Bernardo *et al.*, "Handwritten pattern recognition for early Parkinson's disease diagnosis," *Pattern Recognit. Lett.*, vol. 125, pp. 78–84, Jul. 2019, doi: 10.1016/J.PATREC.2019.04.003.
- [18] S. H. Ismael, S. W. Kareem, and F. H. Almkhtar, "Medical Image Classification Using Different Machine Learning Algorithms," *Mosul Univ.*, vol. 14, no. 1, pp. 135–147, May 2020, doi: 10.33899/CSMJ.2020.164682.
- [19] M. H. M. Alhabib, M. Z. N. Al-Dabagh, F. H. AL-Mukhtar, and H. I. Hussein, "Exploiting Wavelet Transform, Principal Component Analysis, Support Vector Machine, and K-Nearest Neighbors for Partial Face Recognition," *Cihan Univ. Sci. J.*, vol. 3, no. 2, pp. 80–84, Aug. 2019, doi: 10.24086/CUESJ.V3N2Y2019.PP80-84.
- [20] F. H. Almkhtar, "Principal Component Analysis and K-Nearest Neighbor Classifier for Facial Expression Recognition System," *Int. J. Curr. Res. Acad. Rev.*, vol. 6, no. 5, pp. 17–20, May 2018, doi: 10.20546/IJCRAR.2018.605.004.
- [21] H. A. Khan, W. Jue, M. Mushtaq, and M. U. Mushtaq, "Brain tumor classification in MRI image using convolutional neural network," *Math. Biosci. Eng.*, vol. 17, no. 5, pp. 6203–6216, 2020, doi: 10.3934/MBE.2020328.
- [22] R. J. Gillies, P. E. Kinahan, and H. Hricak, "Radiomics: Images Are More than Pictures, They Are Data," *Radiology*, vol. 278, no. 2, pp. 563–577, Feb. 2016, doi: 10.1148/RADIOL.2015151169.
- [23] R. Abdulaali Azeez, M. K. Abdul-Hussein, M. Salih Mahdi, and H. T. S. Alrikabi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Orig. Res.*, vol. 10, no. 1, pp. 178–187, 2022.
- [24] M. G. Galety, F. H. Al Mukthar, R. J. Maarroof, F. Rofoo and S. Arun, "Marking Attendance using Modern Face Recognition (FR): Deep Learning using the OpenCV Method," *2022 8th International Conference on Smart Structures and Systems (ICSSS)*, 2022, pp. 1-6, doi: 10.1109/ICSSS54381.2022.9782265.
- [25] M. Z. AL-Dabagh and D. F. H. AL-Mukhtar, "Breast Cancer Diagnostic System Based on MR images Using KPCA-Wavelet Transform and Support Vector Machine," *Int. J. Adv. Eng. Res. Sci.*, vol. 4, no. 3, pp. 258–263, 2017, doi: 10.22161/IJAERS.4.3.41.
- [26] Y. S. Mezaal and A. S. Al-Zayed, "Design of microstrip bandpass filters based on stair-step patch resonator," <https://doi.org/10.1080/00207217.2018.1545144>, vol. 106, no. 3, pp. 477–490, Mar. 2018, doi: 10.1080/00207217.2018.1545144.
- [27] X. Fan and M. Jiang, "RetinaFaceMask: A Single Stage Face Mask Detector for Assisting Control of the COVID-19 Pandemic," *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, pp. 832–837, May 2020, doi: 10.48550/arxiv.2005.03950.

- [28] A. F. Al-zubidi, N. F. AL-Bakri, R. K. Hasoun, S. H. Hashim, and H. T. S. Alrikabi, "Mobile Application to Detect Covid-19 Pandemic by Using Classification Techniques: Proposed System," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 16, pp. 34–51, Aug. 2021, doi: 10.3991/IJIM.V15I16.24195.
- [29] J. H. Bappy, A. K. Roy-Chowdhury, J. Bunk, L. Nataraj, and B. S. Manjunath, "Exploiting Spatial Structure for Localizing Manipulated Image Regions," *Proc. IEEE Int. Conf. Comput. Vis.*, vol. 2017-October, pp. 4980–4989, Dec. 2017, doi: 10.1109/ICCV.2017.532.
- [30] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2016-December, pp. 770–778, Dec. 2015, doi: 10.48550/arxiv.1512.03385.
- [31] H. Wang, T. Raiko, L. Lensu, T. Wang, and J. Karhunen, "Semi-Supervised Domain Adaptation for Weakly Labeled Semantic Video Object Segmentation," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10111 LNCS, pp. 163–179, Jun. 2016, doi: 10.48550/arxiv.1606.02280.
- [32] K. A. Ehinger, K. Allen, and J. M. Wolfe, "Change blindness for cast shadows in natural scenes: Even informative shadow changes are missed," *Attention, Perception, Psychophys.*, vol. 78, no. 4, pp. 978–987, May 2016, doi: 10.3758/S13414-015-1054-7/FIGURES/7.
- [33] L. D'Amiano, D. Cozzolino, G. Poggi, and L. Verdoliva, "A PatchMatch-Based Dense-Field Algorithm for Video Copy-Move Detection and Localization," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 3, pp. 669–682, Mar. 2019, doi: 10.1109/TCSVT.2018.2804768.
- [34] H. H. Tseng, L. Wei, S. Cui, Y. Luo, R. K. Ten Haken, and I. El Naqa, "Machine Learning and Imaging Informatics in Oncology," *Oncology*, vol. 98, no. 6, pp. 344–362, Jun. 2020, doi: 10.1159/000493575.
- [35] A. Asthana, S. Zafeiriou, S. Cheng, and M. Pantic, "Incremental face alignment in the wild," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, pp. 1859–1866, Sep. 2014, doi: 10.1109/CVPR.2014.240.
- [36] C. Liu, Y. Wang, K. Kumar, and Y. Gong, "Investigations on speaker adaptation of LSTM RNN models for speech recognition," *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, vol. 2016-May, pp. 5020–5024, May 2016, doi: 10.1109/ICASSP.2016.7472633.
- [37] A. Ullah, S. M. Anwar, M. Bilal, and R. M. Mehmood, "Classification of Arrhythmia by Using Deep Learning with 2-D ECG Spectral Image Representation," *Remote Sens.*, vol. 12, no. 10, May 2020, doi: 10.3390/rs12101685.
- [38] B. N. Mohammed, F. H. Al-Mukhtar, R. Z. Yousif, and Y. S. Almashhadani, "Automatic Classification of Covid-19 Chest X-Ray Images Using Local Binary Pattern and Binary Particle Swarm Optimization for Feature Selection," *Cihan Univ. Sci. J.*, vol. 5, no. 2, pp. 46–51, Nov. 2021, doi: 10.24086/CUESJ.V5N2Y2021.PP46-51.
- [39] I. A. Aljazaery, H. ALRikabi, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International Journal of Online Biomedical Engineering*, vol. 18, no. 3, pp. 101-113, 2022.
- [40] J. Hernandez-Ortega, J. Fierrez, A. Morales, and J. Galbally, "Introduction to Presentation Attack Detection in Face Biometrics and Recent Advances," Nov. 2021, doi: 10.48550/arxiv.2111.11794.
- [41] X. Li, J. Komulainen, G. Zhao, P. C. Yuen, and M. Pietikainen, "Generalized face anti-spoofing by detecting pulse from face videos," *Proc. - Int. Conf. Pattern Recognit.*, vol. 0, pp. 4244–4249, Jan. 2016, doi: 10.1109/ICPR.2016.7900300.
- [42] H. Salim, S. H. Abbood, M. S. Rahim, and A. M. Alaidi, "DR-LL Gan: Diabetic Retinopathy lesions synthesis using Generative Adversarial Network," *International journal of online and biomedical engineering*, vol. 18, no. 3, 2022.
- [43] J. Tang et al., "Image edge detection based on singular value feature vector and gradient operator," *Math. Biosci. Eng. 2020 43721*, vol. 17, no. 4, pp. 3721–3735, May 2020, doi: 10.3934/MBE.2020209.
- [44] M. K. Abdul-Hussein, I. Obod, and I. Svyd, "Evaluation of the Interference's Impact of Cooperative Surveillance Systems Signals Processing for Healthcare," *International journal of online and biomedical engineering*, vol. 18, no. 3, 2022.
- [45] X. Shi, Z. Chen, H. Wang, D. Y. Yeung, W. K. Wong, and W. C. Woo, "Convolutional LSTM Network: A Machine Learning Approach for Precipitation Nowcasting," *Adv. Neural Inf. Process. Syst.*, vol. 2015-January, pp. 802–810, Jun. 2015, doi: 10.48550/arxiv.1506.04214.