Deep Learning Algorithm for Face Recognition Using a Hybrid Model

Ahmed Adil Nafea*[1], Mohammed Salah Ibrahim[1], Mohammed M AL-Ani[2], Zainab O. Hama[3]

[1]Department of Artificial Intelligence, College of Computer Science and IT, University of Anbar, Ramadi, Iraq.
[2]Center for Artificial Intelligence Technology (CAIT), Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi, Selangor, Malaysia.
[3]Department of Animal Science, College of Agricultural Engineering Sciences, Sulaimani University, Sulaimani, Iraq.

Abstract **—This study presents a robust hybrid model for face recognition, which synergistically integrates the VGG16 convolutional neural network (CNN) for feature extraction with an autoencoder for dimensionality reduction and representation learning. This paper proposed VGG16 and Autoencoder architecture efficiently extracts high-level features from images, much reducing computational complexity while the classify of the extracted features used Support Vector Machine (SVM). The proposed hybrid model has achieved a high accuracy of 98% in face recognition tasks on benchmark datasets. This high accuracy highlights efficiency of combination VGG16-based feature extraction with autoencoder of a dimensionality reduction technique and SVM classification in advancing the state-of-the-art in face recognition approaches.**

Key words: - Face recognition, Deep learning, Machine learning, Classification, Detection

Introduction

Face recognition is important field in the domain of computer vision and biometric detection [1]. The increasing challenge for secure authentication systems in several areas like surveillance, access control, and mobile applications, there is a critical need for accurate and efficient face recognition algorithms [2], [3]. Deep learning (DL) techniques have shown a leading model in computer vision, representing high performance in many tasks, including object recognition, image classification, and face recognition [4], [5].

VGG16 is a recognized architecture in the scope of DL, known for its ability to extract complex features from images. Its efficiency the high-dimensional feature vectors produced via VGG16 can be computationally intensive and may contain redundant information. So, to address these issues and enhance the discriminative power of the extracted features, dimensionality reduction techniques like autoencoders have been applied. Autoencoders are unsupervised neural networks proposed to encode the input data into a lower-dimensional representation crack it back to the primary data, while minimizing the reconstruction error.

This paper proposed a novel hybrid model for face recognition of mixes the feature extraction capabilities of the VGG16 with the dimensionality reduction and representation learning of an autoencoder. The proposed VGG16-Autoencoder hybrid architecture goals to extract high-level features from facial images efficiently and reduce the computational complexity of subsequent processing to classify the extracted features and perform the final recognition, an SVM classifier is applied. SVMs are recognized for their robustness, efficiency, and ability to handle high-dimensional data, making them a good choice for classification tasks in face recognition systems. The objective of this work is to proposed hybrid model in enhancing the accuracy of face recognition systems.

This paper is organized as following section: In Section 2 talk about review of related works in the area of face recognition. While Section 3 explains details the methodology, including the VGG16-Autoencoder hybrid model and SVM classifier. But Section 4 shows the discussion and experimental results. Finally, Section 5 shows concludes the paper.

Related work

The fast development of Generative Adversarial Networks (GANs) presents a new challenge for anti-forensics face approaches. GANs can generate false photos and videos, possibly leading to identity theft and privacy violations. This paper develops a deep CNN to detection physical faces utilizing GANs to generate fictitious faces in several sizes and resolutions. The network is fine-tuned for classifying authentic and false images, with promising results from AI Challenge validation data [6].

Image forensics is essential for addressing online deception campaigns and social media issues. In the recent advancements focus on detecting GANs like 'deepfakes', which can generate synthetic imagery identical from real images. The structure of a GAN implementation's generating network can reveal a large difference in coverage treatment from a real camera, enabling effective discrimination between GAN imagery and real camera images utilized to train the GAN [7].

Advancements in computer vision and image processing have made it easier to manipulate original images without detection, especially in face regions. User-friendly software like Photoshop and Meitu allow manipulation without authorization and can be shared online. Face detection and recognition techniques are essential in distinguishing between real and fake images. DL technology has proposed advanced

DOI:http://doi.org/10.24086/cocos2024/paper.1572

image-to-image translating approaches, but traditional methods like ELA, local noise features, and CFA are insufficient [8].

The paper discusses the identification of deep network generated (DNG) images, highlighting the difference among camera image and DNG generation image. It proposes a feature set to capture color image statistics for DNG identification and evaluates detection situations like mismatched training data and real images. Experiments show the proposed technique accurately identifies DNG images and outperforms existing approaches, especially when the GAN model is unknown [9].

This paper evaluated various face detection and recognition models on Android devices. Google ML Kit showed the best results, taking only 68 milliseconds as standard to identify a face. FaceNet was the most accurate, with a high accuracy of 95% for most instances. MobileFaceNet was the fastest, taking only 90 milliseconds on average to produce and output. A face recognition application was developed utilizing the excellent models performing [10].

The study proposes a CNN algorithm to detect fake images on social media, particularly in politics and celeb circles. The algorithm includes preprocessing images, gamma correction, and Canny filter extraction. It employs Principal Component Analysis (PCA) and CNN without PCA. The results show that using PCA provides acceptable accuracy, while CNN only achieves the highest level of accuracy at 86.5 in detecting manipulated images [11].

This paper proposes a new deepfake detection schema using SVM and CNN, along with a publicly available dataset called 140k Real and Fake Faces. Technological advancements have led to the rise of deepfakes, which can replace real faces with computer-generated ones, spreading mass misinformation. The model can correctly detect deepfakes in images, and accuracy rates of 88.33% [12].

Research Methodology

The proposed model for human shape detection uses a hybrid approach, combining VGG16 with an auto-encoder for feature extraction and SVM as a classifier. The framework includes preprocessing, dataset development, feature extraction, and classification. The methodology and significance of each phase are explained as shown in Figure 1.

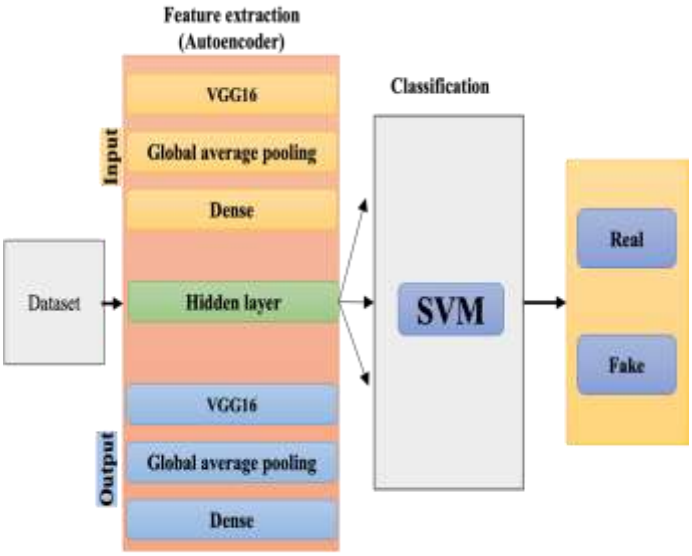

Figure. 1. Research Methodology

DATASET DISCRIBTION

Deepfake detection systems use binary classifiers to group fake and real information. A dataset from Kaggle contains 70k real and 70k fake faces from Flickr and Bojan's 1 Million fake faces. This proposed utilized two features as images and labels. The labeling one as fake and label zero as real, to Deepfake image classifiers [13]. As shown in Figure 2 dataset sample.

Figure. 1. Dataset sample

AUGMENTATION

The augmented stage is to applying transformations of the dataset, like rotation, scaling, flipping, and shifting, to increase its variation and improve the model's ability. This method additionally addresses limited data issues via generating new augmented samples [14],[15].

FEATURE EXTRACTION

The study proposed a hybrid feature extraction model via combining the VGG16 with an autoencoder to enhance feature

DOI:http://doi.org/10.24086/cocos2024/paper.1572

extraction abilities and reduce computational complexity in face recognition. The VGG16 is ability to extract complex features from images, while the autoencoder is an unsupervised neural network architecture that encodes input data into a lower-dimensional latent space and rebuilds it back to primary data with minimal loss. This combination of improving feature extraction's discriminative power, robustness, and efficiency, leading to improved recognition accuracy.

SUPPORT VECTOR MACHINES (SVM)

SVM is a supervised learning algorithm utilized for regression and classification tasks [16],[17]. It is classifies high-level features from images into different classes based on individual identities [18]. The SVM's basic theory is to find the optimal hyperplane that maximally splits data points of unique classes in the feature space, minimizing classification error in binary classification problems [19],[20].

The hybrid model of VGG16-Autoencoder as a feature extraction is input for the SVM classifier which learns to classify images into real and fake classes.

EVALUATION

The study evaluated a system's accuracy using metrics like recall, precision, accuracy, and F-score [21]. Precision measures positive instances detected, recall measures correctly identified positive instances, and accuracy measures correctly classified instances [22]. The F-measure integrates precision and recall [23].

$$F - measure = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (1)$$

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \quad (3)$$

$$Recall = \frac{TP}{TP + FN} \quad (4)$$

Result and discussion

This section shows the results of the hybrid model of VGG16 with autoencoder as a feature extraction to improve face recognition detection, specifically in real and fake. In Table 1, the proposed model has achieved highest accuracy of 98%.

Table 1 : proposed results

0	precision	recall	f1-score	support
fake	0.96	1.00	0.98	10000
real	1.00	0.96	0.98	10000
accuracy			**0.98**	20000
macro avg	0.98	0.98	0.98	20000
weighted avg	0.98	0.98	0.98	20000

As shown in Figure 3 a confusion matrix of proposed hybride model.

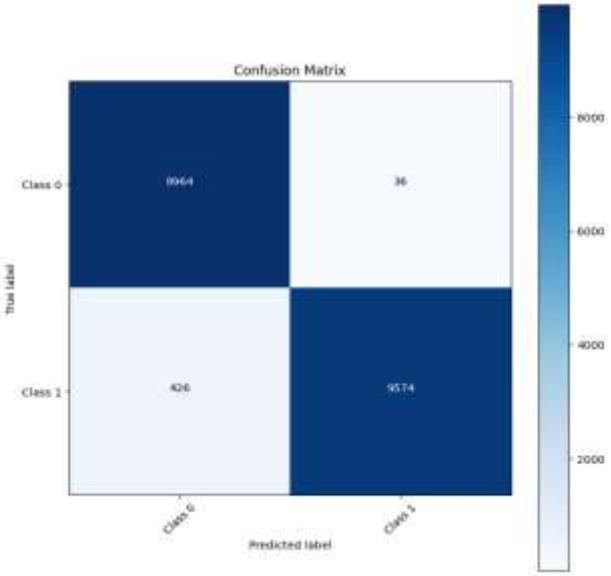

Figure. 3. confusion matrix using proposed hybride model

As shown in Figure 4 a ROC curve of hybride proposed model.

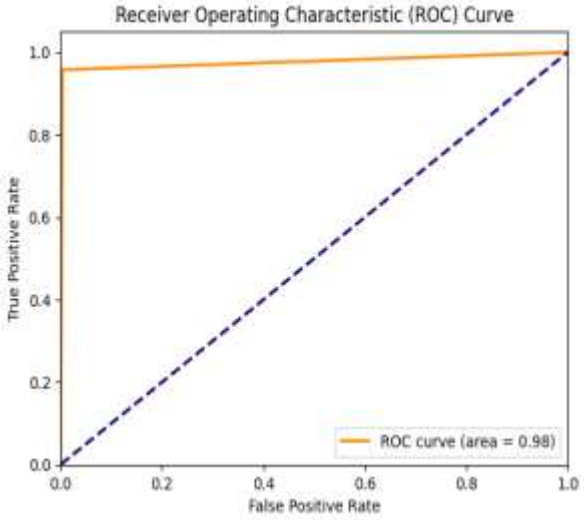

Figure. 4. ROC curve

Its important to compare our study with state of the art studies.This study [11] used a CNN with PCA and achieved an accuracy of 86.5%. This research [12] has used CNN and SVM and achieved an accuracy of 88.33%. This paper [6] has used a GAN and acquired an accuracy of 80%. In this proposed [10] utilized MobileFaceNet models has achieved an

DOI:http://doi.org/10.24086/cocos2024/paper.1572

accuracy of 95%. This study [8] proposed DL technique and acquired an accuracy of 90.76%. In this research [9] proposed DNG and acquired an accuracy of 96%. In this research [7] proposed GAN and acquired an accuracy of 70%. Depending on the hybrid proposed model it is clear that the proposed hybrid approach is yet considered to be competitive.

In Figure. 5 shows a comparison between the hybrid approach with related work studies.

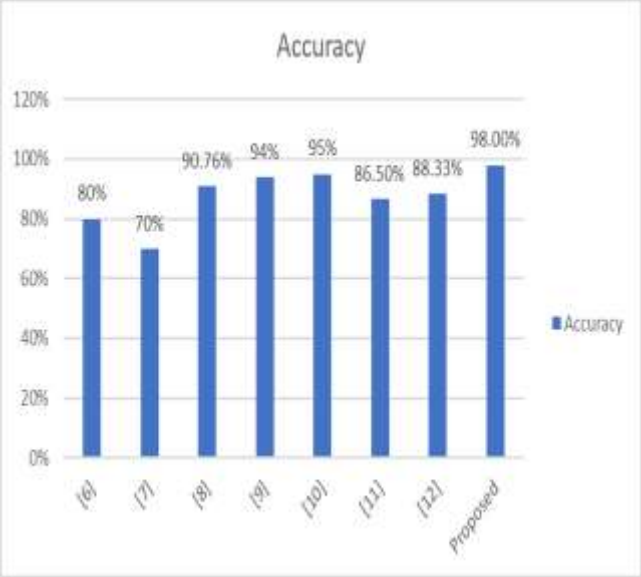

Figure. 5. A comparison results between the proposed work and related work

Conclusion

In this study, we proposed a novel hybrid model for face recognition by integrating the feature extraction capabilities of the VGG16 convolutional neural network (CNN) with an autoencoder for dimensionality reduction and representation learning. The extracted features were classified using a Support Vector Machine (SVM) classifier. The experimental results on benchmark face recognition datasets demonstrated the effectiveness of the proposed hybrid model, achieving an impressive accuracy rate of 98%. Compared to traditional DNN-based and conventional face recognition methods, the hybrid model showcased improved recognition accuracy and robustness, validating the potential of integrating deep CNN-based feature extraction with dimensionality reduction techniques and SVM classification in advancing face recognition systems. In future work recommend to Incorporating Advanced Deep Learning Techniques: Exploration of advanced deep learning architectures, such as Residual Networks (ResNets) or Transformer-based models, could further enhance the feature extraction capabilities and robustness of the hybrid model.

Referencess

[1] S. Hangaragi, T. Singh, and N. Neelima, "Face detection and Recognition using Face Mesh and deep neural network," *Procedia Comput. Sci.*, vol. 218, pp. 741–749, 2023.

[2] A. Sardar, S. Umer, R. K. Rout, S.-H. Wang, and M. Tanveer, "A secure face recognition for IoT-enabled healthcare system," *ACM Trans. Sens. Networks*, vol. 19, no. 3, pp. 1–23, 2023.

[3] M. A. S. Ali, M. Meselhy Eltoukhy, F. Rajeena PP, and T. Gaber, "Efficient thermal face recognition method using optimized curvelet features for biometric authentication," *PLoS One*, vol. 18, no. 6, p. e0287349, 2023.

[4] A. A. Nafea, S. A. Alameri, R. R. Majeed, M. A. Khalaf, and M. M. AL-Ani, "A Short Review on Supervised Machine Learning and Deep Learning Techniques in Computer Vision," *Babylonian J. Mach. Learn.*, vol. 2024, pp. 48–55, 2024.

[5] L. Jiao and J. Zhao, "A survey on the new generation of deep learning in image processing," *Ieee Access*, vol. 7, pp. 172231–172263, 2019.

[6] N.-T. Do, I.-S. Na, and S.-H. Kim, "Forensics face detection from GANs using convolutional neural network," *ISITC*, vol. 2018, pp. 376–379, 2018.

[7] S. McCloskey and M. Albright, "Detecting GAN-generated imagery using saturation cues," in *2019 IEEE international conference on image processing (ICIP)*, 2019, pp. 4584–4588.

[8] L. Wen and D. Xu, "Face image manipulation detection," in *IOP conference series: materials science and engineering*, 2019, vol. 533, no. 1, p. 12054.

[9] H. Li, B. Li, S. Tan, and J. Huang, "Identification of deep network generated images using disparities in color components," *Signal Processing*, vol. 174, p. 107616, 2020.

[10] S. Hettiarachchi, "Analysis of different face detection andrecognition models for Android." 2021.

[11] H. Sabah, "A Detection of Deep Fake in Face Images Using Deep Learning," *Wasit J. Comput. Math. Sci.*, vol. 1, no. 4, pp. 94–111, 2022.

[12] J. Mallet, L. Pryor, R. Dave, and M. Vanamala, "Deepfake detection analyzing hybrid dataset utilizing cnn and svm," in *Proceedings of the 2023 7th International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence*, 2023, pp. 7–11.

[13] J. Sharma, S. Sharma, V. Kumar, H. S. Hussein, and H. Alshazly, "Deepfakes Classification of Faces Using Convolutional Neural Networks.," *Trait. du Signal*, vol. 39, no. 3, 2022.

[14] O. J. Kadhim, A. A. Nafea, S. A. S. Aliesawi, and M. M. Al-Ani, "Ensemble Model for Prostate Cancer Detection Using MRI Images," in *2023 16th International Conference on Developments in eSystems Engineering (DeSE)*, 2023, pp. 492–497.

[15] K. Alomar, H. I. Aysel, and X. Cai, "Data augmentation in classification and segmentation: A survey and new strategies," *J. Imaging*, vol. 9, no. 2, p. 46, 2023.

[16] A. A. Nafea, M. Mishlish, A. M. S. Shaban, M. M. AL-Ani, K. M. A. Alheeti, and H. J. Mohammed, "Enhancing Student's Performance Classification Using Ensemble Modeling," *Iraqi J. Comput. Sci. Math.*, vol. 4, no. 4, pp. 204–214, 2023.

[17] A. Kurani, P. Doshi, A. Vakharia, and M. Shah, "A comprehensive comparative study of artificial neural network (ANN) and support vector machines (SVM) on stock forecasting," *Ann. Data Sci.*, vol. 10, no. 1, pp. 183–208, 2023.

[18] N. N. Jamil and A. K. Kareem, "Comparative Analysis on Machine Learning and One-Dimensional Convolutional Neural Network to Predict Surface Enhanced Raman Spectroscopy," in *2023 3rd International Conference on Computing and Information Technology (ICCIT)*, 2023, pp. 216–221.

[19] M.-C. Kim, J.-H. Lee, D.-H. Wang, and I.-S. Lee, "Induction motor fault diagnosis using support vector machine, neural networks, and boosting methods," *Sensors*, vol. 23, no. 5, p. 2585, 2023.

[20] A. A. Nafea, M. S. Ibrahim, A. A. Mukhlif, M. M. AL-Ani, and N. Omar, "An Ensemble Model for Detection of Adverse Drug Reactions," *ARO-THE Sci. J. KOYA Univ.*, vol. 12, no. 1, pp. 41–47, 2024.

[21] K. M. A. Alheeti, A. Alzahrani, M. Alamri, A. K. Kareem, and D. Al_Dosary, "A Comparative Study for SDN Security Based on Machine Learning.," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 11, 2023.

[22] H. J. Mohammed, A. A. Nafea, H. K. Almulla, S. A. S. Aliesawi, and M. M. Al-Ani, "An Effective Hybrid Model for Skin Cancer Detection Using Transfer Learning," in *2023 16th International Conference on Developments in eSystems Engineering (DeSE)*, 2023, pp. 840–845.

[23] A. K. Kareem and K. M. A. Alheeti, "Hybrid Approach for Fall Detection Based on Machine Learning," in *International Conference on New Trends in Information and Communications Technology Applications*, 2021, pp. 111–130.

DOI:http://doi.org/10.24086/cocos2024/paper.1572