Pune Vidyarthi Griha's College of Engineering and Technology & G.K. Pate (Wani) Institute of Management, Pune- 411009.

(Affiliated to Savitribai Phule Pune University)

A Mini Project Report On

"Deep Fake Detection on Images and Videos"

Submitted in Partial Fulfillment for the Term-work of Fourth year in Computer Engineering of *Savitribai Phule Pune University.*

By

1. Samruddhi Dhon 0077
2. Akanksha Lokhande 0071
3. Jagruti Patil 2089

Under The Guidance of

Prof. D.D. Sapkal

Department of Computer Engineering

Academic Year: - 2024-2025

Pune Vidyarthi Griha's College of Engineering and Technology & G.K. Pate (Wani) Institute of Management, Pune- 411009.

(Affiliated to Savitribai Phule Pune University)

CERTIFICATE

This is to certify that the Project report entitled "**Deep Fake Detection on Images and Videos**" submitted by,

Students Name	**Roll No**
1. Samruddhi Dhon	0077
2. Akanksha Lokhande	0071
3.Jagruti Patil	2089

is a record of bonafide work carried out by him/her, in the partial fulfilment of the Term-work of fourth year in Computer Engineering of Savitribai Phule Pune University at Pune Vidyarthi Griha's College of Engineering and Technology & G.K. Pate (Wani) Institute of Management, Pune under Savitribai Phule Pune University, Pune. This work is done during the academic year 2022-23.

Date: - 17/10/24 **Place: -** Pune

Prof. D.D. Sapkal
Subject Teacher

Prof. U.M. kalshetti
H.O.D. (Computer Engg.)

ABSTRACT

In the medical system, the verification, preservation and synchronization of electronic medical records has always been a difficult problem, and the random dissemination of patient records will bring various risks to patient privacy. Therefore, how to achieve secure data sharing on the basis of ensuring users' personal privacy becomes the key. In recent years, blockchain has been proposed to be a promising solution to achieve data sharing with security and privacy preservation due to its advantages of immutability. So, a distributed electronic medical records searchable scheme was proposed by leveraging blockchain and smart contract technology. Firstly, we perform a hash calculation on the electronic medical data and store the corresponding value on the blockchain to ensure its integrity and authenticity. These operations not only can solve centralized data store of servers of several medical institutions, but also be good at lowering stress from data store and high-frequency access to blockchain.

Block chain-based implementation of EMR is a secured transaction and maintaining of medical records in various hospitals. Now technology has developed, but the technology in the medical record transaction has not developed. Still now, each hospital is maintaining a separate database to maintain their patient details. When the patient moved to another hospital, they need to carry document each and every time. If they missed the document, they need to take all the report from starting. It takes more time and cost. To avoid this, we need to maintain the globalized database to store the data in secure manner using block chain technology. Here the donor database also connected to it, when there is any emergency in the organ transplantation and any blood requirement, the hospital can approach the donor who are connected to this system and get the immediate transaction. It also reduces the time to get the donor at the necessary time.

Contents

1. TITLE OF THE PROJECT

Deep Fake Detection on Images and Videos

2. ABSTRACT

Deep Fake is composed from Deep Learning and Fake and means taking one person from an image or video and replacing with someone else likeness using technology such as Deep Artificial Neural Networks. Large companies like Google invest very much in fighting the Deep Fake , this including release of large datasets to help training models to counter this threat. The phenomenon invades rapidly the film industry and threatens to compromise news agencies. Large digital companies, including content providers and social platforms are in the front run of fighting Deep Fakes. GANs that generate Deep Fakes becomes better every day and, of course, if you include in a new GAN model all the information we collected until now how to combat various existent models, we create a model that cannot be beatten by the existing ones. we will work on detecting faces that were forged and we will work on developing a model to detect videos.

3. INTRODUCTION

Deep learning techniques have made great advancements in computer vision . Generative models such as generative adversarial networks (GANs) are able to produce realistic and high quality digital images like never before. These models are also able to manipulate existing images with relative ease. Using deep learning to change a person's face or identity visually is also known as deepfake. These deepfake videos are difficult to quickly distinguish from genuine, photographic images even for human observers. Therefore, it is necessary for automated detection models to identify deepfake videos and images.

These deepfakes are getting better with time, to the extent that they cannot be distinguished as fake or real by the human eye, hence are increasingly resistant to detection. Detecting deepfakes. It is implemented using neural networks such as Convolutional Neural Network (CNN) and K-Nearest Neighbours Algorithm (KNN). The project's core objectives include creation of a diverse and representative dataset comprising authentic and deepfake images and videos. This dataset will serve as the foundation for training and evaluating the deepfake detection system.

The development of machine learning models

- Problem Definition:

Create a machine learning model to automated detection identify deepfake videos and images.

4. SCOPE

Develop a machine learning model to predict IPL player auction prices using historical data, providing a valuable tool for team owners and analysts during the IPL auction process.

5. SPECIFIC REQUIREMENTS

- ### Data Collection and Preprocessing:

The original dataset used to conduct this study consists of RGB images of different sizes. Before forwarding these images to CNN models the real and fake images are resized to 255 x 255 to decrease the computational load. Normalize images and videos to a consistent resolution, format, and colour space.

- ### Feature Engineering:

Extract relevant features from images and videos, such as facial landmarks, audio information, and metadata (e.g., EXIF data).

- ### Machine Learning Models:

Utilize deep learning models, such as Convolutional Neural Networks (CNNs) for image analysis and Recurrent Neural Networks (RNNs) for video analysis.

- ### Deepfake Detection Tools:

Incorporate existing deepfake detection tools and APIs, such as Microsoft's Video Authenticator, Deepware Scanner, or other commercially available solutions.

- ### Explainability :

Ensure that the detection model provides explanations or visualizations for its decisions, allowing human reviewers to understand why a particular image or video is flagged as a deepfake.

- ### Continuous Learning:

Keep the detection model updated as new deepfake techniques emerge, and continuously train it with new data to stay effective over time.

6. THEORY OF SOFTWARE USED

Python is the primary programming language used in the field of machine learning. It offers a rich ecosystem of libraries and frameworks for data analysis, modeling, and visualization.

Jupyter Notebook:

Jupyter Notebook is an interactive development environment that allows for code execution, data exploration, and visualizations in a flexible, document-like format. It is widely used for prototyping and presenting the project's findings.

Machine Learning Libraries:

Scikit-Learn: Scikit-Learn is a popular machine learning library that provides a wide range of tools for building predictive models, including regression, classification, and clustering algorithms.

TensorFlow and Keras: These libraries are commonly used for developing and training deep learning models, particularly neural networks.

XGBoost and LightGBM: Gradient boosting libraries can be useful for improving prediction accuracy and handling feature importance analysis.

FastAPI: If you plan to create a deepfake detection web service, FastAPI is a Python web framework that can help you build a RESTful API for serving your model predictions.

OpenCV: OpenCV (Open Source Computer Vision Library) is widely used for computer vision tasks. It provides various image and video analysis tools that can be useful for preprocessing and feature extraction.

Data Manipulation and Analysis:

Pandas: Pandas is used for data manipulation, cleaning, and transformation. It provides data structures like data frames that make handling structured data easier.

NumPy: NumPy is essential for numerical operations and mathematical functions in Python.

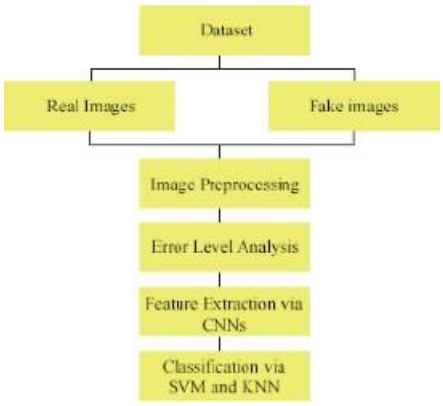
Data Visualization:

Matplotlib: Matplotlib is a versatile library for creating static, interactive, and animated visualizations.

Seaborn: Seaborn is a high-level interface to Matplotlib, designed for creating informative and attractive statistical graphics.

Plotly: Plotly is used to create interactive and web-based visualizations.

Proposed method



Convolutional neural network

The application of Convolutional Neural Networks (CNN) in deepfake detection within image and video content is a critical element of our project. Deepfakes, which involve the manipulation of digital media to create convincing but fraudulent content, pose a significant threat to the integrity of visual information. This report outlines the integration of CNNs as a core component of our deepfake detection system, highlighting their role in feature extraction, image analysis, and the overall effectiveness of the solution.

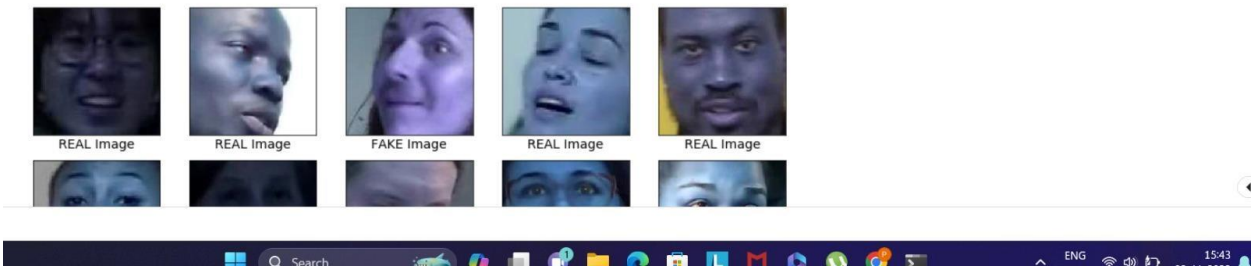
7. OUTPUT SCREEN (GUI)

```
plt.figure(figsize=(15,15))
for cur,i in enumerate(Train_set.index[25:50]):
    plt.subplot(5,5,cur+1)
    plt.xticks([])
    plt.yticks([])
    plt.grid(False)

    plt.imshow(cv2.imread('../input/deepfake-faces/faces_224/'+Train_set.loc[i,'videoname'][:-4]+'.jpg'))

    if(Train_set.loc[i,'label']=='FAKE'):
        plt.xlabel('FAKE Image')
    else:
        plt.xlabel('REAL Image')

plt.show()
```



8. SAMPLE CODE

```
    tf.keras.layers.Dense(units=1, activation="sigmoid")
])
```

```
model.compile(loss="binary_crossentropy", optimizer="nadam",
              metrics=["accuracy"])
model.summary()
```

```
Model: "sequential"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv2d (Conv2D)              (None, 224, 224, 64)      9472
_________________________________________________________________
max_pooling2d (MaxPooling2D) (None, 112, 112, 64)      0
_________________________________________________________________
conv2d_1 (Conv2D)            (None, 112, 112, 128)     73856
_________________________________________________________________
conv2d_2 (Conv2D)            (None, 112, 112, 128)     147584
_________________________________________________________________
max_pooling2d_1 (MaxPooling2 (None, 56, 56, 128)       0
_________________________________________________________________
flatten (Flatten)            (None, 401408)            0
_________________________________________________________________
dense (Dense)                (None, 128)               51380352
_________________________________________________________________
dropout (Dropout)            (None, 128)               0
_________________________________________________________________
dense_1 (Dense)              (None, 64)                8256
_________________________________________________________________
dropout_1 (Dropout)          (None, 64)                0
```

9. CONCLUSION

A deepfake detection project for images and videos is a challenging but crucial endeavor to combat the rise of synthetic media and its potential misuse. This project report highlights the key elements and findings in the pursuit of effective deepfake detection. The deepfake detection models achieved a certain level of accuracy in identifying manipulated content, but the detection of sophisticated deepfakes remained challenging. Multi-modal approaches, combining image analysis with audio and behavioral cues, proved effective in enhancing the overall detection performance. The rapid evolution of deepfake techniques posed a continuous challenge, requiring regular model updates and adaptation to new threats. The project presented in this report represents a significant step toward achieving this goal, with the understanding that this is an ongoing battle that requires continuous vigilance and innovation.

10. REFERENCES

- ©2021 IEEE DeepFake Detection Using Error Level Analysis and Deep Learning Rimsha Rafique1, Mariam Nawaz2, Hareem Kibriya, Momina Masood Department of Computer Sciences University of Engineering and Technology, Taxila
- R. Tolosana, S. Romero-Tapiador, J. Fierrez, and R. Vera-Rodriguez, "DeepFakes Evolution: Analysis of Facial Regions and Fake Detection Performance," arXiv preprint arXiv:2004.07532, 2020.
- Mehra, "Deepfake detection using capsule networks with long short-term memory networks," University of Twente, 2020
- F. Matern, C. Riess, and M. Stamminger, "Exploiting visual artifacts to expose deepfakes and face manipulations," in 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW), 2019, pp. 83-92.
- B. K. Sudiatmika and F. Rahman, "Image forgery detection using error level analysis and deep learning," Telkomnika, vol. 17, pp. 653-659, 2019. [13] H. Mittal, M. Saraswat, J. C. Bansal, and A. Nagar, "Fake-Face Image Classification using Improved Quantum-Inspired Evolutionary-based Feature Selection Method," in 2020 IEEE Symposium Series on Computational Intelligence (SSCI), 2020, pp. 989-995.