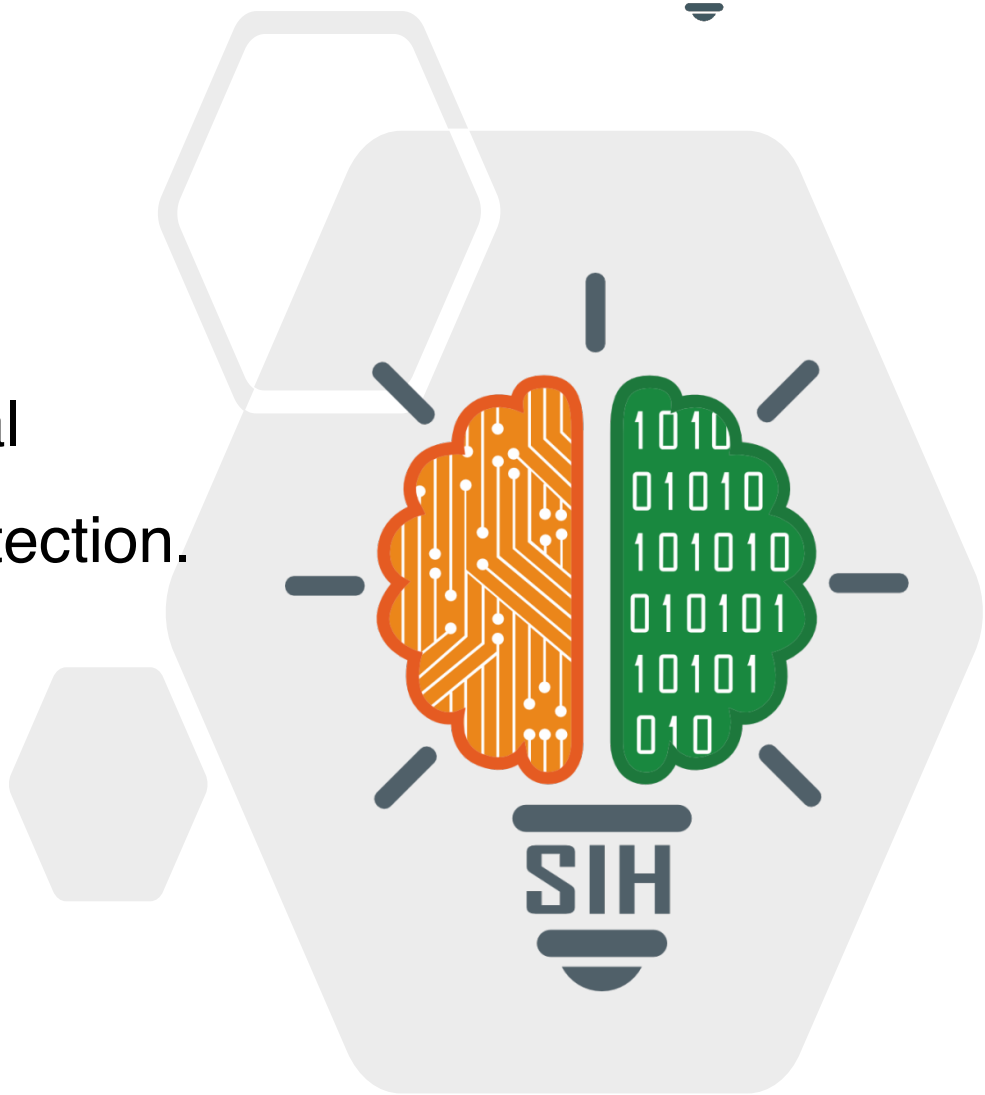
SMART INDIA HACKATHON 2024

TITLE PAGE

- **Problem Statement ID –** 1671
- **Problem Statement Title-** Develop a functional solution that demonstrates the face liveness detection.
- **Theme-** Smart Automation
- **PS Category-** Software
- **Team ID-**
- **Team Name-** Code Crushers



CODE CRUSHERS

FACE LIVENESS DETECTION

SMART INDIA HACKATHON 2024

❖ Proposed Solution:

A deep-learning pipeline capable of spotting fake vs legitimate faces and performing anti-face spoofing in face recognition systems. It is built with the help of keras, Tensorflow, and OpenCV.

❖ Addressing the Problem:

Challenge: High-quality spoofing techniques, such as deepfakes and high-resolution masks, make it difficult to distinguish between real and fake faces.

Solution: Combine pre-trained models with custom neural network layers and temporal dynamics to detect subtle discrepancies. Feature extraction and a tailored classification head help the model learn nuanced liveness indicators.

❖ Innovation and Uniqueness:

Explainable AI: Implementing explainability techniques enhances the trustworthiness of the model by providing insights into its decision-making process.

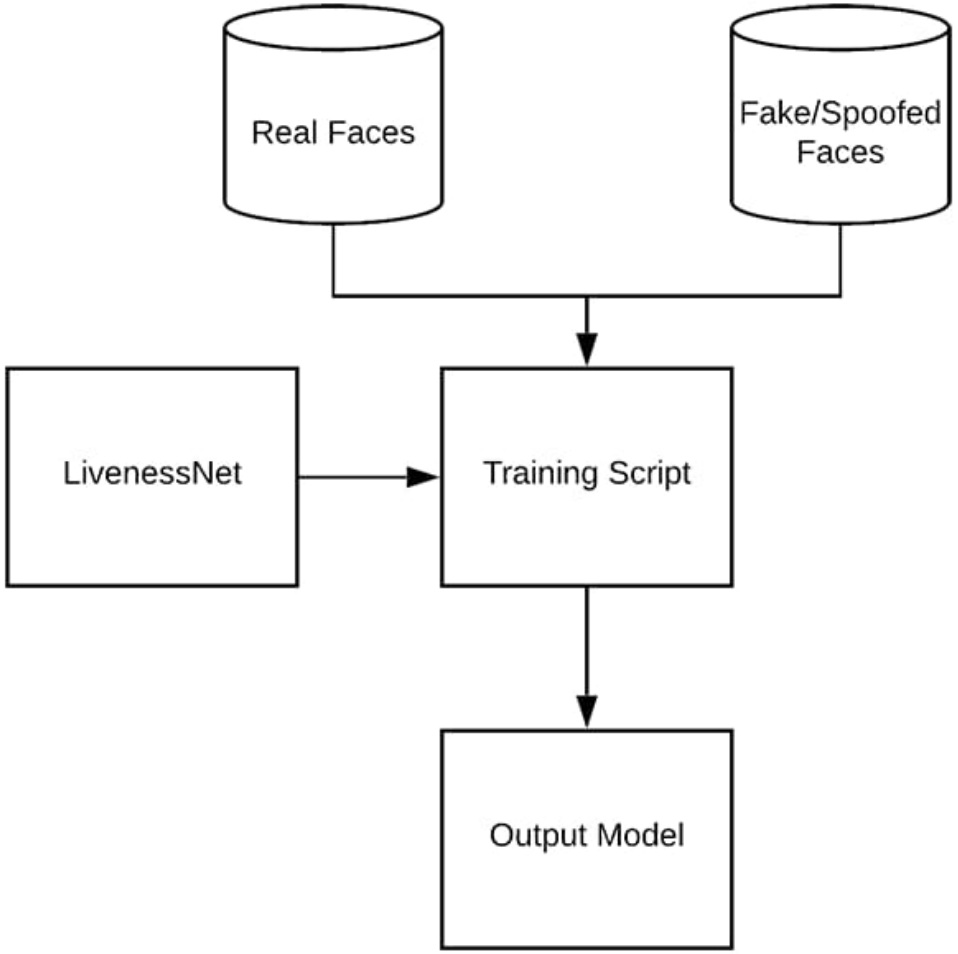
Multi-Modal Integration: Leveraging both deep learning and texture-based methods improves robustness against various spoofing techniques.

CODE CRUSHERS

TECHNICAL APPROACH

SMART INDIA HACKATHON 2024

- It is built with the help of Keras, Tensorflow, and OpenCV.
- **Sample_liveness_data:** contains the sample dataset.
- **Deploy.prototxt:** Support file for pre-trained face detector.
- **Deploy.prototxt:** Support file for pre-trained face detector.
- **Es10_300x300_ssd_iter_140000.caffemodel:** Pre-trained face detector.
- **Train_liveness.py:** The python script to train the model.
- **Optical Flow Analysis:** For capturing motion dynamics in video sequences.



CODE CRUSHERS

FEASIBILITY AND VIABILITY

SMART INDIA HACKATHON 2024

❖ Feasibility Analysis:

The feasibility of a deep-learning pipeline for detecting fake faces is high due to advances in technology and available datasets. Challenges include handling diverse spoofing techniques and ensuring real-time accuracy. Success depends on robust training and adaptability to new spoofing methods.

❖ Potential Challenges:

Potential challenges include managing the diversity of spoofing methods and ensuring the system performs well in real-time scenarios. Risks involve overfitting to specific spoofing techniques and the potential for adversarial attacks that could bypass detection.

❖ Overcoming Challenges:

To overcome these challenges, use a diverse and extensive dataset that includes a wide range of spoofing techniques to ensure robust training. Implement regularisation techniques and cross-validation to prevent overfitting. Incorporate real-time testing and iterative updates to adapt to emerging spoofing methods.

CODE CRUSHERS

IMPACT AND BENEFITS

SMART INDIA HACKATHON 2024

- **Impact on Environment:** Efficient deep-learning algorithms can reduce computational resource requirements and energy consumption, contributing to lower carbon footprints for data centers.

- **Benefits to Mankind:** By improving face recognition security, the project helps protect personal identity and sensitive information, reducing fraud and enhancing safety in various applications.

- **Day-to-Day Life:** The technology ensures more reliable and secure access controls, such as unlocking devices or authorising transactions, and boosts user confidence in digital interactions by minimising the risk of identity theft.

CODE CRUSHERS

RESEARCH AND REFERENCES

SMART INDIA HACKATHON 2024

❖ Existing solutions and case studies:

~ Samsung’s Face Recognition for Mobile Devices.
~ Microsoft Azure Face API.
~ University of Oxford's Liveness Detection System.

❖ Privacy and Compliance considerations:

~ "Privacy-Preserving Face Recognition Using Deep Learning Techniques" by E. A.T. Lee et al..
~ "Adversarial Attacks and Privacy Concerns in Face Recognition Systems" by S. Shum et al.