Terrier Cyber Quest 2024 Datathon: Track 3

Territorial Army Cyber Challenge: Innovating for the Future of Defense

Prototype Title-THE DEEPFAKE SLAYER

Team Name: bornpresident

• Team Member 1 • Name: Vishal Chand • email id: vishalchand20016@gmail.com • Mobile No: +91-7717363942	Team Member Name 2: • Name: Aditya Singh • email id: adsingh837@gmail.com • Mobile No:+91-9838980461

THE DEEPFAKE SLAYER

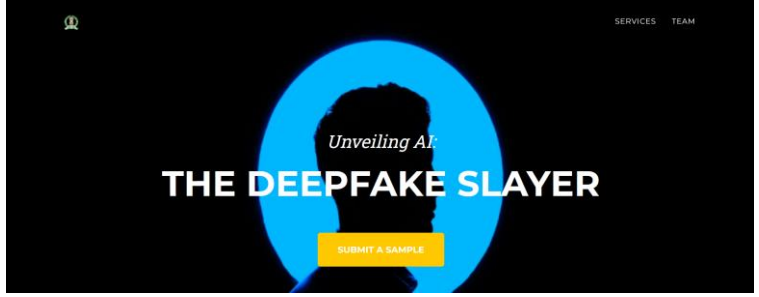
TERRIER CYBER QUEST 2024

Audio Detection
Mel-Frequency Cepstral Coefficients (MFCC)

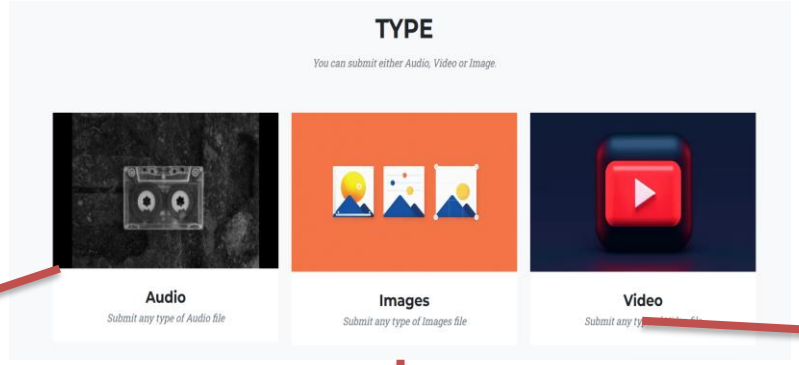
Solution

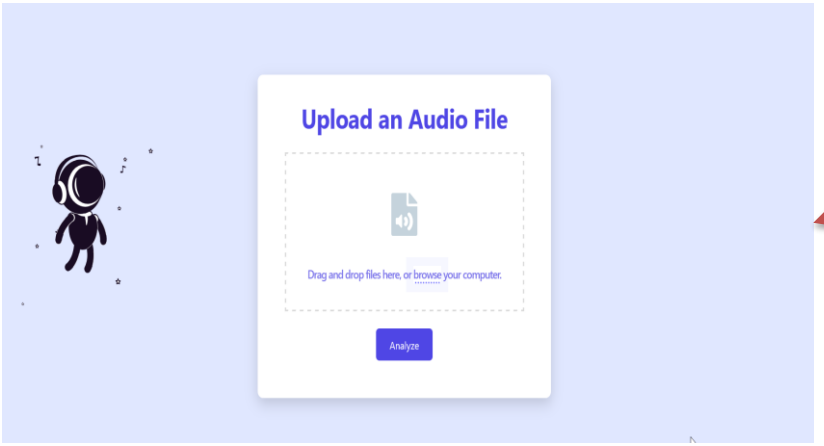
Video Detection
Deep Learning(ResNext and LSTM)

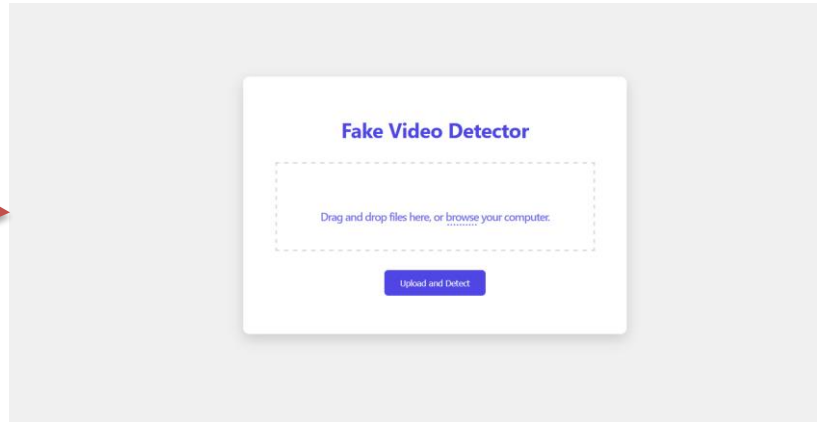
Image Detection
Using CNN (Built using TensorFlow & Keras)

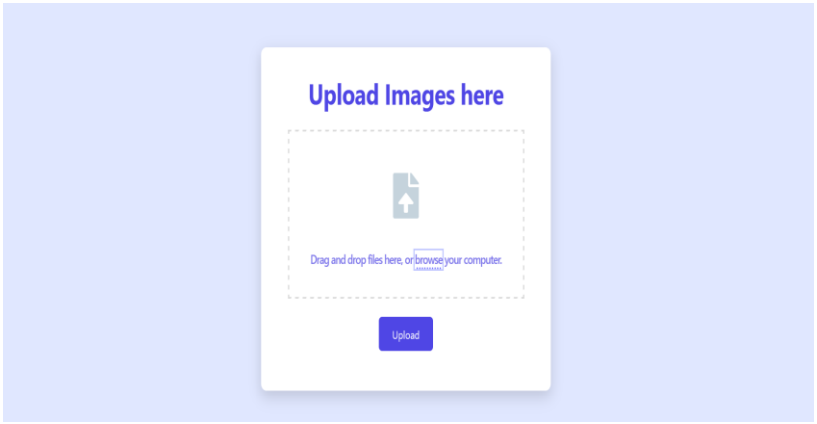


TERRIER CYBER QUEST 2024









Innovation & Uniqueness

TERRIER CYBER QUEST 2024

•Supports various file types

•Reporting feature to Indian law enforcement agencies.

•URL submission

•Feedback loop for **automated learning**.

•Informative dashboards for visual analytics.

Technologies used

- **Programming languages:** Python, JavaScript
- **Machine learning libraires:** PyTorch,TensorFlow, Keras, scikit-learn, NumPy, pandas, Matplotlib,etc
- **Hardware**: CPU/GPU-enabled systems for model training interference

❖ AI/ML Algorithm used

- **Audio detection:** MFCC, SVM, Random Forest, MLP, XGBoost.
- **Image detection:** CNN using TensorFlow and Keras.
- **Video detection: CNN & RNN**

Feasibility, Challenges, and Strategies

TERRIER CYBER QUEST 2024

Feasibility:

•**Audio Detection**: The project uses MFCC (Mel-frequency cepstral coefficients) features extracted from audio files and a Support Vector Machine (SVM) classifier to differentiate between genuine and deepfake audio.

•**Video Detection**: ResNext & LSTM architectures suited for deepfake video analysis.

•**Image Detection**: CNN (TensorFlow/Keras) ideal for image manipulation detection.

Challenges & Risks:

•**Data Quality**: Difficulty in sourcing large, clean, labeled deepfake datasets.

•**Generalization**: Models might struggle with unseen deepfakes.

•**Real-time Performance**: Potential latency for large video files.

•**Model Complexity**: High computational requirements for complex models.

Strategies to Overcome:

•**Data Quality**: Leverage synthetic data generation & data augmentation.

•**Generalization**: Use transfer learning to adapt to new datasets.

•**Real-time Performance**: Optimize models with lightweight/quantized versions.

•**Model Complexity**: Utilize cloud computing & hardware accelerators (GPUs/TPUs).

TERRIER CYBER QUEST 2024

Impact & Benefits

Law Enforcement:
Button click reporting,quick identification of deepfakes,aiding investigations

General Public: Increases trust in online content

Media:Content intergrity

Impact on target audience

Government: National Security

Content Creator: Protect against deepfake misuse

Economic:
Helps prevent fraud, safeguardingbusinesses and financial sectors from deepfake scams.

Social:
Reduces misinformation, protecting individual reputations and public trust.

Benefits

Technological: Fight against fake content, driving innovation in cybersecurity.

RESEARCH AND REFERENCES

TERRIER CYBER QUEST 2024

- https://github.com/abhijitjadhav1998/Deepfake_detection_using_deep_learning
- https://github.com/talreiss/factor
- https://abhijithjadhav.medium.com/deepfake-video-detection-using-long-short-term-memory-df3674f83ecc
- https://arxiv.org/abs/2107.14480
- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9996362
- **Data-set references :**

✓ https://www.kaggle.com/datasets/manjilkarki/deepfake-and-real-images

✓ https://github.com/yuezunli/celeb-deepfakeforensics

✓ https://www.kaggle.com/c/deepfake-detection-challenge/data

✓ https://github.com/ondyari/FaceForensics