ENNOBLE IP
Sets Knowledge Through Action

Marwadi University

INVENTION DISCLOSURE FORM FOR PATENTS

Applicant Name-Marwadi University

1. **Particulars of Inventors**

Mr./Ms/Dr.	Name (Full)	Department	Designation	Mobile No.	Email	Postal Address
Mr	Yashkumar mayani	CE	Student	8469324380	yashkumarmyani@gmail.com	Rajkot
Mr	Pradip Chavada	CE	Student	9316071998	pradip.chavada123491@marwadiuniversity.ac.in	Rajkot
Ms	Reshma Sunil	CE	Professor	6358256076	reshma.sunil@marwadieducation.edu.in	Rajkot

2. **Provide title of the invention: Deepfake detection in image using ML**

3. **In 100 words or less, please provide an abstract or summary of the invention: This work benchmarks five CNN architectures—ResNet, EfficientNet, MobileNet, Xception, and DenseNet—for detecting deepfake images. Using a curated 512×512 dataset from FaceForensics++ and other sources, all models were trained under identical settings with uniform preprocessing. Evaluation metrics include accuracy, precision, recall, F1-score, and inference time. Findings show a balance between detection accuracy and computational efficiency, guiding model selection for real-time deepfake detection in social media and forensic applications.**

4. **Detail description of the invention:(Answer to all below are required in detail)**

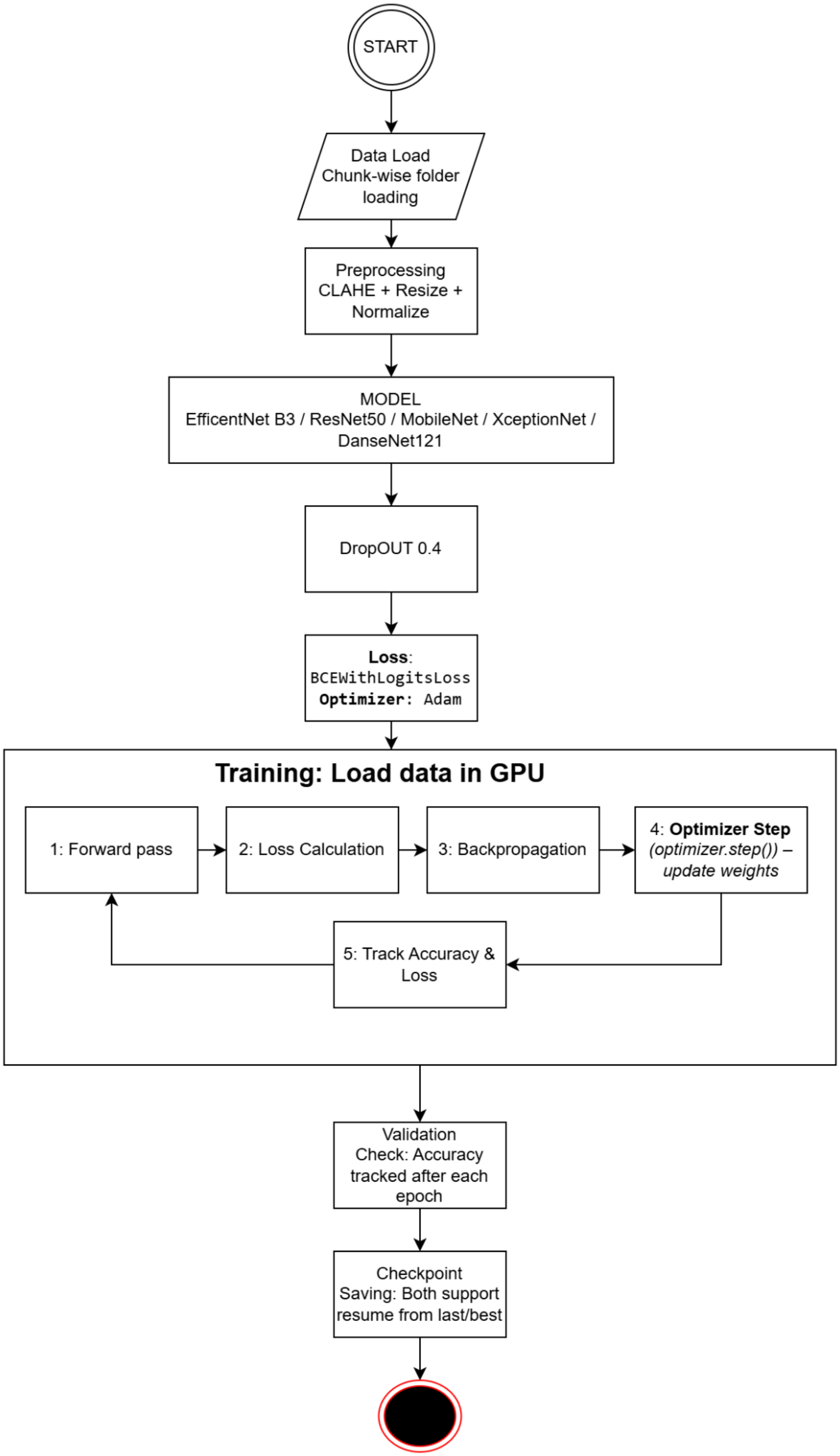
   a. **Problem the invention is solving**
   Deepfake Identity misuse

   b. **General Utility/application of the invention**
   Froud protection

   c. **Advantages of the invention disclosing about the increased efficiency/efficacy**
   Faster and trusted

   d. **Best way of using the invention as well as possible variants**
   On image data for classification anyhow

   e. **Working of invention along with Drawing, schematics and flow diagrams if required with complete explanations**


START
Data Load
Chunk-wise folder
loading
Preprocessing
CLAHE + Resize +
Normalize
MODEL
EfficentNet B3 / ResNet50 / MobileNet / XceptionNet /
DanseNet121
DropOUT 0.4
Loss: BCEWithLogitsLoss
Optimizer: Adam
Training: Load data in GPU
1: Forward pass
2: Loss Calculation
3: Backpropagation
4: **Optimizer Step** *(optimizer.step()) – update weights*
5: Track Accuracy & Loss
Validation
Check: Accuracy
tracked after each
epoch
Checkpoint
Saving: Both support
resume from last/best

The flowchart represents the training pipeline for deepfake image classification using CNN architectures. The process begins with chunk-wise data loading, followed by preprocessing steps such as CLAHE for contrast enhancement, resizing, and normalization. The preprocessed images are then fed into one of the selected models—EfficientNet B3, ResNet50, MobileNet, XceptionNet, or DenseNet121—with a dropout rate of 0.4 to prevent overfitting. Training is performed on GPU, where a forward pass generates predictions, the loss is calculated using BCEWithLogitsLoss, and backpropagation updates weights through the Adam optimizer. Accuracy and loss are tracked during each iteration. After every epoch, validation checks are conducted to monitor performance, and model checkpoints are saved, supporting both the last and best versions for resuming training.

5. **Have you conducted Primary Patent Search? Yes / No (if yes, attach the patent search results)**
   This is research project not patent based innovation.

6. **Existing state-of-the-art and prior arts: (Brief background of the existing knowledge/product/process in the market)**
   This is not final product, it can be a part of final product.

7. **List out the known ways about how others have tried to solve the same or similar problems? Indicate the disadvantages of these approaches. In addition, please identify any prior art documentation or other material that explains or provides examples of such prior art efforts.**

Traditional Visual & Handcrafted Features

- **Method: Detects artefacts like inconsistent eye blinking, head movement, lip-sync mismatch, lighting, or compression noise.**
- **Disadvantages:**
  - **Fragile → fails when forgeries are high-quality.**
  - **Easily bypassed with newer GAN-based models (StyleGAN, DeepFaceLab).**

Frequency & Spectrum Domain Analysis

- **Method: Detects anomalies in image frequency spectrum or JPEG compression traces.**
- **Disadvantages:**
  - **Not robust when fakes are re-compressed or filtered.**
  - **Can misclassify real images with editing or compression artefacts.**

Classical Machine Learning (SVM, Random Forests)

- **Method: Uses handcrafted features (texture, color histograms, head pose) and ML classifiers.**
- **Disadvantages:**
  - **Limited feature learning capacity.**
  - **Poor generalization across datasets and manipulation methods.**

CNN-based Deep Learning Models

- **Method: ResNet, Xception, VGG-based CNNs trained to classify real vs fake.**
- **Disadvantages:**
  - **Dataset-specific → models overfit to certain forgeries.**
  - **High computational cost for large-scale or real-time detection.**

Temporal Models (RNN, LSTM, 3D CNN)

- **Method: Exploits video temporal inconsistencies (eye blinks, micro-expressions).**
- **Disadvantages:**
  - **Requires long video sequences, not suitable for single-image fakes.**
  - **Expensive in memory and computation.**

Transformer-based Approaches (Vision Transformers, multimodal BERT-like models)

- **Method: Uses attention mechanisms to capture global inconsistencies.**
- **Disadvantages:**
  - **Very data-hungry, needs massive training datasets.**
  - **High inference time, limiting real-time deployment.**

Biometric/Physiological Signal Detection

- **Method: Detects subtle cues like heartbeat from facial skin colour changes, or micro-movements.**
- **Disadvantages:**
  - **Requires high-quality, high-frame-rate video.**
  - **Fails with low-resolution or compressed social media videos.**

S. No.	Existing state of art	Drawbacks in existing state of art	Overcome (how your invention is overcoming the drawback)
1	Handcrafted Feature-based Methods (eye blink, head pose, lip-sync mismatch, noise patterns)	Fragile; fails against high-quality GAN-based forgeries; dataset-specific.	Using CNN architectures (ResNet, EfficientNet, MobileNet, Xception, DenseNet) to automatically learn robust features beyond handcrafted rules.
2	Frequency & Spectrum Domain Approaches (FFT, JPEG artefact detection)	Sensitive to compression, filtering, or re-encoding; prone to false positives on real but compressed media.	Preprocessing pipeline (CLAHE, normalization, resizing) ensures consistent input quality and reduces dependence on compression artefacts.
3	Classical ML Models (SVM, Random Forests) with handcrafted features	Limited capacity; poor generalization across datasets/manipulation types.	Deep CNNs with dropout and uniform training conditions improve generalization across diverse manipulations.
4	CNN-based Detection (e.g., Xception, VGG, ResNet)	Risk of overfitting to specific datasets; high	Comparative evaluation of multiple CNNs highlights

		computational cost in real-time use.	trade-offs between accuracy and efficiency, allowing selection of optimal models for real-time deployment.
5	Temporal/Video-based Models (RNN, LSTM, 3D CNNs)	Require long video sequences; memory intensive; not suitable for single images.	Focuses on single-image deepfake detection with optimized CNNs for lightweight, faster inference.
6	Transformer-based Approaches (ViT, multimodal models)	Very data-hungry; high training and inference cost; not practical for small-scale use.	Uses efficient CNNs (EfficientNet, MobileNet) to balance accuracy and computational efficiency, making them deployable in real-time scenarios.
7	Biometric/Physiological Signal-based Detection (heartbeat, skin tone changes)	Needs high-resolution, high-frame-rate videos; unreliable on social media content.	Our approach works on 512×512 still images, making it applicable to both low- and high-quality data from real-world sources.

8. **List the Technical features and Elements of the invention along with the Description of your invention from start to end.**

The invention begins by loading image data in chunks **to handle large-scale datasets efficiently. Each image undergoes** preprocessing **steps, including CLAHE for enhanced contrast, resizing to 512×512, and normalization for stable training. Preprocessed data is then passed into one of several CNN models (EfficientNet-B3, ResNet50, MobileNet, XceptionNet, DenseNet121), with a** dropout rate of 0.4 **to avoid overfitting.**

Training proceeds on a GPU**, where images are processed through the model in a** forward pass**, followed by** loss calculation **using BCEWithLogitsLoss. Gradients are updated via** backpropagation**, and model weights are optimized with the** Adam optimizer**. At each iteration,** accuracy and loss are tracked**.**

After every epoch, the system performs a validation check **to evaluate the model's generalization on unseen data. Performance is measured using standard metrics such as accuracy, precision, recall, F1-score, and inference time, ensuring both detection quality and efficiency.**

Finally, the system includes a checkpointing mechanism **to save both the latest and best-performing models, enabling easy recovery and further training if needed. This ensures the invention provides a** scalable, efficient, and reliable framework **for deepfake image classification in real-world applications such as** social media monitoring and forensic analysis**.**

9. **List out the features of your invention which are believed to be new and distinguish them over the closest technology.**
   New Comparative outcome for Deepfake Detection on Different CNNs
10. **Has the invention been built or tested or implemented? If yes please provide the Efficiency/Efficacy details of the invention**
    It has be developed and tested and its deep learning project.

Metric	EfficientNet-B3	DenseNet121	Xception-Net	ResNet50	MobileNet
Epoch	17	16	11	16	10
Test Accuracy	99.95%	99.94%	99.85%	99.78%	99.63%
Fake Precision	~1.000	0.9999 / ~1	0.9997	~0.999	~0.999
Fake Recall	~0.9996	0.9999 / ~1	0.9974	~0.999	~0.999
FFHQ Precision	~0.9996	~0.9999	0.997	~0.999	~0.999
FFHQ Recall	~1.000	~0.9999	0.9997	~0.999	~0.999
Misclassified	15	~18	~44	~66	~110
Training Accuracy	~100%	~100%	99.80%	99.99%	99.35%
Validation Accuracy	99.96%	99.92%	99.83%	99.81%	99.45%
Training Loss	~0	~0	0.0001	0.0017	0.0012
Model Size	123 MB	80.5 MB	238 MB	269 MB	25.8 MB

11. **Briefly state when and how you first conceived this idea?**
    I first conceived this idea around 4–5 months ago while exploring recent advances in computer vision and the growing concern around deepfake media. During my review of existing detection techniques, I noticed that many approaches either overfit to specific datasets or were too computationally heavy for real-time use. This observation led me to design a framework that systematically compares multiple CNN architectures under uniform conditions, with a focus on balancing detection accuracy and efficiency.
12. **Have you sold, offered for sale, publicly used or published anything related to this invention? If yes, please briefly explain the dates and circumstances. List those individuals to whom you have revealed your invention. Were non-discloser documents signed prior to discloser in each case? Please state any deadlines of which you may be aware for filing an application on this invention.**
    NO.

13. **Include any reasons that your invention would not have been obvious to someone of average skill in the art.**
    This invention would not have been obvious to someone of average skill because it requires specialized knowledge in Machine Learning and Deep Learning, along with a clear understanding of deepfake generation techniques and their impacts. An average person without this background would not be -

able to design a comparative framework, select suitable CNN architectures, apply uniform preprocessing, or evaluate trade-offs between accuracy and efficiency. Moreover, the approach is not straightforward—it involves extensive hit-and-trial experimentation, consuming significant computational resources, time, and careful planning to achieve reliable results.

14. Additional comments by inventor (if you want to give more details out of scope of this IDF).
This is just the beginning. As AI continues to advance, deepfakes will become even more sophisticated, and the current models may not remain as effective as they are today. A promising direction would be to extend this work into a reinforcement learning environment, where models can continuously adapt and improve against evolving manipulation techniques, providing a more resilient and long-term solution.