

Minor Project - 6th Semester

Team Members:

- Riyanish Chouhan – ID: 22U02013
- Vikas Kaushik – ID: 22U02036

Supervised by: Prof. Ajay Kumar Shrivastava,
Training & Placement Officer (TPO)

Project Coordinator: Dr. Yatendra Sahu,
Department of Computer Science & Engineering,
IIIT Bhopal (M.P.)

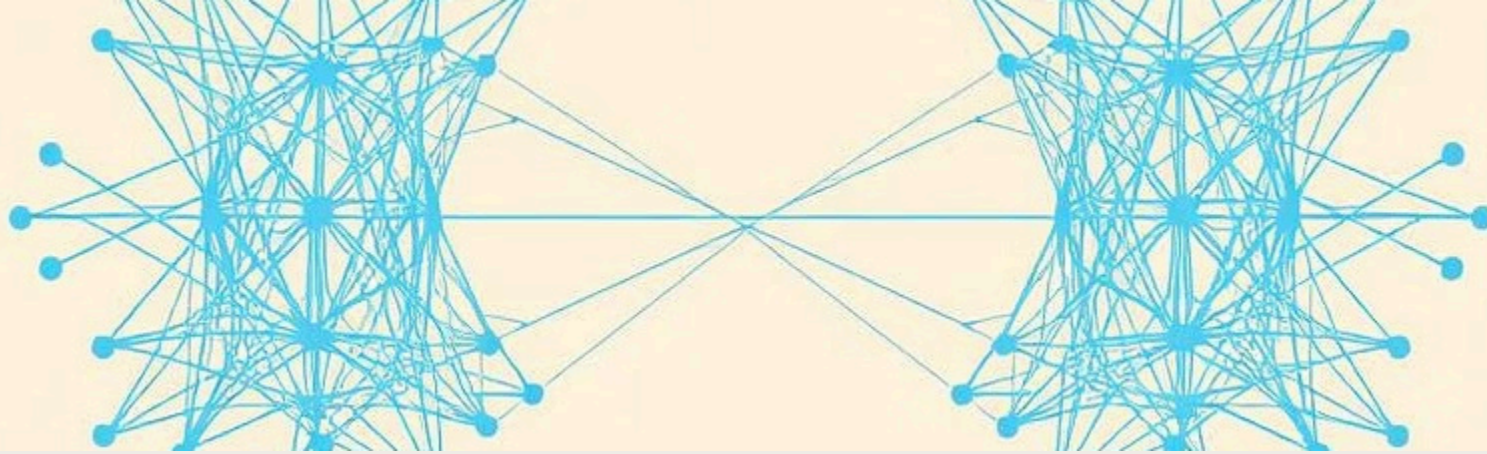
ID Card Tampering Detection using OpenCV and Deep Learning (Siamese Networks)

This web-based system accurately detects tampering in ID cards by analyzing subtle differences between original and altered images.

It combines traditional pixel-level image analysis with OpenCV and advanced deep learning techniques, leveraging Siamese Networks to compare pairs of ID card images and identify inconsistencies.

Siamese Networks excel at learning similarity metrics, enabling the detection of even the smallest modifications that may indicate tampering.

The integration of these technologies creates a highly reliable detection system ideal for security screening, identity verification, and fraud prevention applications.



Literature: Siamese Networks and Image Matching

Siamese Networks

- **Siamese Networks** learn to measure similarity between two inputs.
- Utilize **twin CNN branches with shared weights** for feature extraction.
- Compare image pairs to produce a **similarity score**.
- Highly effective at detecting **subtle differences** often missed by conventional models.
- Widely used for applications such as **tampering detection, signature verification, and facial recognition**.

OpenCV

- **OpenCV** facilitates **automated image comparison** between original and tampered ID cards.
- Executes **pixel-level analysis** to identify discrepancies.
- **Highlights altered regions** using red bounding boxes.
- Enhances verification processes for **identity validation, border security, and fraud prevention**.
- **Reduces human error** and **speeds up processing**.
- **Streamlines and scales** manual inspection workflows effectively.
- Improves overall **accuracy** and **efficiency** in authenticity checks.

Problem Statement and Project Objectives

Problem

ID card tampering threatens identity verification.

Objective 1

Detect tampering via pixel comparison and deep learning.

Objective 2

Provide similarity scores for tampering detection.

Objective 3

Deploy Siamese Network for enhanced accuracy.



Methodology: OpenCV and Siamese Network Workflow

1

OpenCV Comparison

- Preprocesses images using OpenCV.
- Converts images to grayscale.
- Computes pixel-wise difference to find discrepancies.
- Applies thresholding to isolate tampered regions.

2

Siamese Network

- Uses Siamese Network with shared-weight CNNs.
- Extracts deep features from both images.
- Calculates Euclidean distance between feature vectors.
- Detects subtle tampering based on image similarity.

3

Output

- Combines OpenCV analysis with deep learning output.
- Uses similarity score to assess likelihood of tampering.
- Provides a clear, interpretable tampering decision.

Implementation Tools and Environment

Backend

- Python, Flask
- OpenCV for image processing
- TensorFlow/Keras for deep learning

Frontend

- HTML, CSS, JavaScript
- Bootstrap for responsive design
- Optional server-side Jinja2 templates

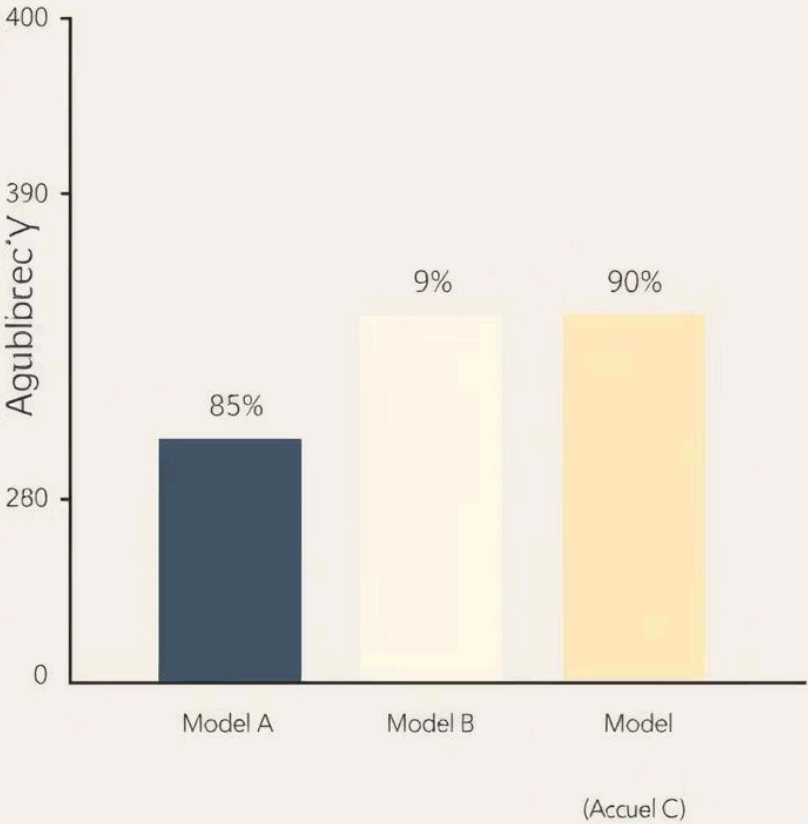
Model


Siamese Network for image similarity-based tampering detection

Comparative Result Analysis of Models

Model	Accuracy
Siamese Network	97.5%
CNN Classifier	91.3%
Triplet Network	93.1%
Vision Transformer	92.8%
ResNet50 + Distance	90.5%

"The ID nnting attows!"
Model-Ilearning detection





Conclusion & Future Directions

Conclusion

The Siamese Network exhibits outstanding capability in tampering detection, delivering high accuracy alongside a lightweight design ideal for real-time deployment. Its proficiency in discerning subtle image differences enables dependable identification of even the most minor modifications, outperforming conventional approaches. Consequently, it stands as a robust and efficient technology suited for securing ID card verification systems.



Future Enhancements

- Expand the dataset by applying synthetic augmentation techniques to improve model generalization and robustness against a broader range of tampering methods.
- Integrate cloud storage solutions for scalable and faster image comparisons, facilitating remote and distributed tampering detection.
- Create tampering heatmaps to visually highlight altered regions, enhancing interpretability and providing clearer evidence for decision-making.
- Investigate additional imaging modalities, such as infrared or ultraviolet, to detect tampering beyond the visible spectrum.
- Further optimize the network architecture to reduce computational load while maintaining or enhancing detection accuracy.