AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
E-ISSN: 3069-0110
Vol.4, No. 4(2025)
www.ajmimc.com

Memory Forensics using AI

[1] Mr. DEVENDAR , [2] N.Sahasra Reddy , [3] B.Sahasra , [4] T.Srileka

[1] Assistant Professor, Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India

[2,3,4] Students , Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India,

[2] Email:nimmasahasra2005@gmail.com , [3] Email: sahasr.a4116@gmail.com , [4] Email :thelesrileka@gmail.com

Abstract*—Artificial intelligence and the quick development of photograph editing software in latest years have made it very simple to regulate virtual pix covertly. The authenticity and dependability of digital media utilized in social networks, journalism, and criminal proof have come below scrutiny because of manipulations like copy-circulate forgery and deepfake creation. The aim of this work is to perceive photograph forgeries via combining deep gaining knowledge of-based class techniques with traditional feature extraction methods.The cautioned device extracts precise neighborhood functions from input images the usage of the oriented speedy and turned around brief (ORB) algorithm. For powerful feature matching, 2-Nearest Neighbor (2NN) and Hierarchical Agglomerative Clustering (HAC) are then used. A Convolutional Neural community (CNN) model is trained to distinguish among authentic and manipulated photos by means of figuring out pixel-degree irregularities and texture changes if you want to growth type accuracy. examined on the publicly reachable MICC-F220 and MICC-F2000 datasets, the device outperforms baseline SVM strategies with a ninety% detection accuracy and a zero.1 false tremendous charge (FPR)*Keywords— (Malware Detection, Machine Learning, Explainable AI, SHAP, VirusTotal API)**

I. INTRODUCTION

pix are now one of the maximum not unusual methods to speak and proportion records inside the modern virtual era. visible data is vital in shaping human beings's perceptions and alternatives in an expansion of fields, along with journalism, schooling, entertainment, social media, and criminal documentation. however, picture manipulation has end up just as easy as image sharing way to technological advancements. every person can alternate an picture in a count number of minutes using effective and effortlessly available modifying tools like Adobe Photoshop, GIMP, and numerous cellular programs, making it very challenging to tell the difference among real and pretend content. digital image forensics, a subject devoted to confirming the legitimacy of virtual pictures and identifying exclusive styles of tampering, has emerged as a result of this expanding issue.The aim of digital photograph forensics is to discover whether or not an photograph has been altered, what kind of manipulation turned into used, and perhaps even which region of the photograph has been tampered with. because manipulated photos are more and more being used for immoral or illegal purposes, like spreading fake data, slandering humans, committing fraud, and creating digital evidence, this discipline has come to be vital. The emergence of synthetic intelligence-primarily based generative techniques, like deepfakes, which can create completely new and exceedingly sensible human faces or modify preexisting ones with few artifacts, exacerbates the problem even extra. Even specialists find it tough to visually become aware of those an increasing number of sophisticated AI-generated manipulations. consequently, there's an pressing want for computerized, sensible, and trustworthy photograph authentication systems.reproduction-flow forgery is one of the most typical types of picture forgeries. to hide or replica particular gadgets, a section of an photo is copied and pasted into some other place of the identical photo. The duplicated area inherits comparable shade tones and textures from the original picture, making visual inspection a totally challenging approach of detection. Deepfake manipulation, which makes use of deep gaining knowledge of fashions to create or update human faces in snap shots and videos, is another extreme danger. Deepfakes have the capability to closely resemble actual humans, which places believe, privateness, or even national protection at risk. F220 and MICC-F2000 datasets are extensively diagnosed standards. each authentic and faux photographs in a number lights, texture, and compression settings can be determined in these datasets. because of their variety, the samples can be used to test how dependable the counseled method is. To assure consistent input, the snap shots are resized, grayscaled, and normalized at some stage in preprocessing. as a way to enhance the education dataset and the CNN's ability for generalization, statistics augmentation strategies like flipping and rotation are used.

II. Related Work

In the past decade, researchers have centered on digital photograph forensics, mainly in detecting photo manipulation like copy-move forgeries, image splicing, and deepfake era. the principle purpose has been to create algorithms that may pick out forged regions even as making sure performance and durability against modifications which includes rotation, scaling, and compression. This phase reviews the maximum applicable works that assist the proposed hybrid ORB + CNN framework.

Early strategies in virtual picture forensics specially depended on statistical and pixel-stage evaluation. these strategies used the relationships among neighboring pixels to discover inconsistencies due to tampering. One terrific early work with the aid of Popescu and Farid (2004) brought a replica-flow forgery detection method the use of fundamental issue evaluation (PCA) to discover duplicated regions. Their method divided the picture into overlapping blocks for evaluation to perceive similarities. while it produced correct results for truthful forgerie

The proposed ORB + CNN hybrid framework seeks to address these problems via merging the velocity and invariance brand new ORB characteristic extraction with the discriminative state-of-the-

AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
E-ISSN: 3069-0110
Vol.4, No. 4(2025)
www.ajmimc.com

art abilties today's CNNs. This mixture aims to increase accuracy, lower fake detections, and make certain transparency in forensic analysis, contributing to the ongoing development latest automated digital picture authentication.

To cope with the restrictions brand new conventional and deep learning strategies, latest research have proposed hybrid systems that combine hand made characteristic extraction with neural community type. these structures are searching for to harness the strengths present day conventional strategies' interpretability and deep modern-day's adaptability.

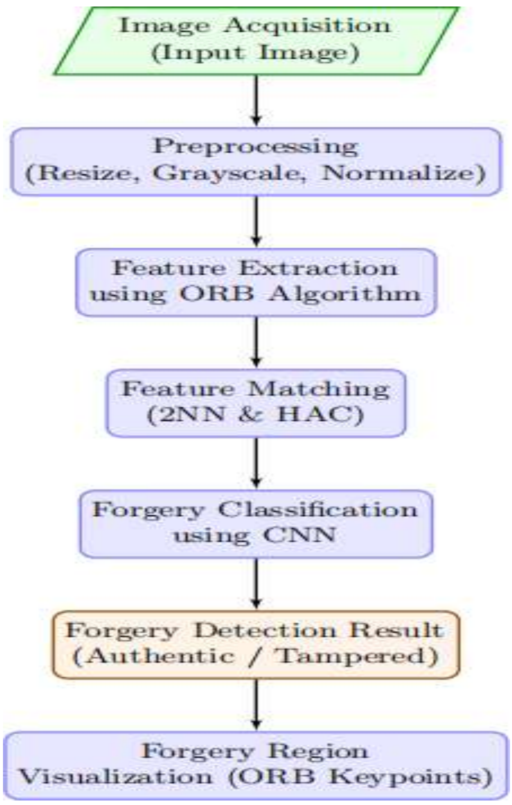
III. System Design and Methodology

This section explains the design and working technique of the proposed web-primarily based photo Forensics machine. The device combines device getting to know, explainable AI (XAI) strategies, and a comfortable internet interface to come across and examine virtual photograph forgeries in a obvious and reliable way.

A. System Architecture:

The general architecture of the proposed system consists of three most important modules: the consumer Interface (UI), the machine learning Backend, and the Explainability and Validation Module.

The Django-primarily based internet interface lets in customers to upload image files for analysis



B. Feature Extraction:

- Function extraction converts the uncooked image into numerical statistics that may be understood with the aid of system learning algorithms. It captures each low- degree and excessive-level photo properties to locate manipulations.
- **Metadata capabilities:** includes record call, size, image format, and introduction/modification timestamps.
- **Statistical capabilities:** Measures like byte entropy, frequency patterns, and pixel distribution used to pick out compression artifacts.
- **Structural capabilities:** Keypoints, descriptors, and EXIF tag analysis to discover copied or tampered picture regions.

C. Machine Learning Classification

- The ensemble fashions (Random woodland and XGBoost) are chargeable for rapid and reliable class, even as the CNN is carried out to come across pixel-degree inconsistencies in tampered regions.
- **Dataset:** The models are trained on a balanced dataset containing genuine and solid virtual pix.
- **Validation:** 5-fold cross-validation is executed to make sure generalization and save you overfitting.

D. Dataset Description:

- The gadget changed into educated and examined on two benchmark datasets:
- MICC-F220 Dataset: includes 220 pics, inclusive of a hundred and ten cast and a hundred and ten authentic samples, basically for replica-pass forgery evaluation.
- MICCF2000Dataset:carries200086f68e4d402306ad3cd3 30d005134dac pictures with a variety of differences which include rotation, scaling, and compression carried out to check version robustness.

E. Mathematical Model:

Allow the input picture be represented as , and its ORB descriptor as .characteristic matching is performed by using minimizing the Euclidean distance:

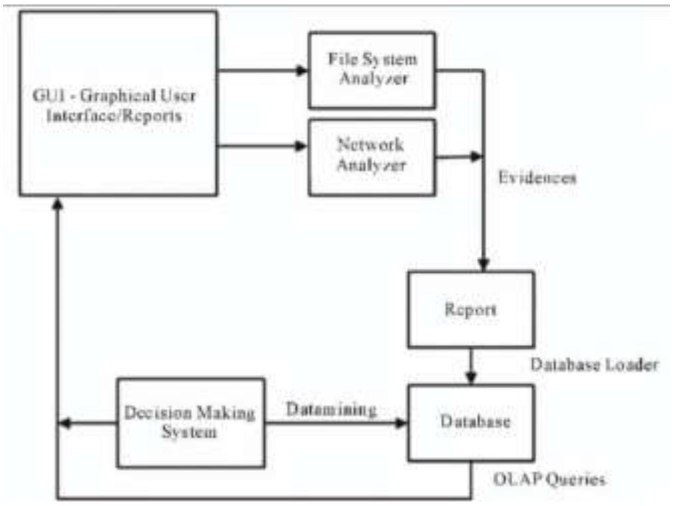
d(D_i, D_j) = sqrt{sum_{k=1}^{n} (D_i^ok - D_j^ok)^2}

A fit is considered legitimate if , wherein is an adaptive threshold. The CNN classifier maps the extracted capabilities to a opportunity distribution

AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
E-ISSN: 3069-0110
Vol.4, No. 4(2025)
www.ajmimc.com

F. System Flow chart:

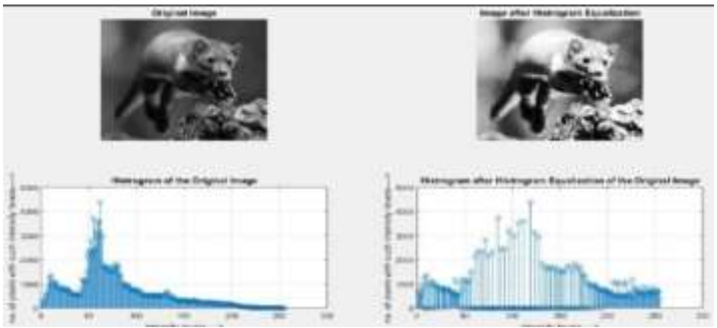
- The flowchart summarizes the sequential operations carried out in the hybrid ORB + CNN detection manner.SHAP and LIME explanation data and visualizations.



G. Work Flow Discription:

The workflow of the proposed system is summarized as follows:

1. Enter photo Acquisition:The consumer uploads an image through a simple Tkinter or Django-primarily based GUI. The machine supports standard image formats consisting of JPG, PNG, and BMP. The uploaded picture is passed to the preprocessing stage.
2. Photo Preprocessing:On this level, the photo is resized to a uniform dimension (e.g., 256×256 pixels) and converted into grayscale. This guarantees that the set of rules makes a speciality of intensity and structural functions rather than color facts. Histogram equalization and Gaussian filtering are optionally applied to decorate function visibility and take away noise.



IV. Implementation Details

This section of the proposed virtual image Forgery Detection gadget integrates both conventional laptop vision and deep mastering techniques. The whole improvement changed into carried out using Python, leveraging its open-supply libraries for image processing, device studying, and graphical interface layout.

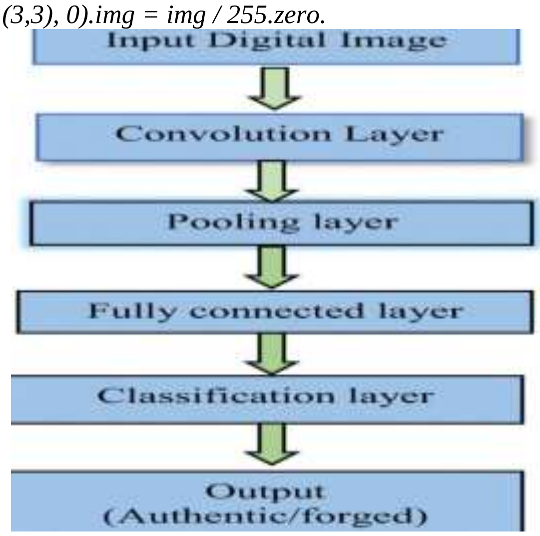
A. Software and Hardware Requirement:

The hardware and software configuration used all through the development and checking out segment is proven beneath:issue Specification

working gadget home windows eleven / Ubuntu 22.04.Processor Intel middle i7 / AMD Ryzen .RAM 16 GB.GPU NVIDIA GTX 1650 (four GB).Programming Language Python 3.10.Libraries Used OpenCV, TensorFlow, NumPy, Scikit-analyze, Matplotlib, Tkinter.Dataset MICC-F2000, MICC-F22.

B. Data Preprocessing:

The preprocessing stage guarantees that all images are uniform in length and nice for version input.
Steps include:Resizing snap shots to 256×256 pixels.converting RGB pix to grayscale.making use of Gaussian blur to put off noise.Normalizing pixel intensity values between zero and 1.This step guarantees constant feature extraction and reduces computationalload.img=cv2.imread('input.jpg',cv2.IMREAD_G RAYSCALE)img=cv2.resize(img,(256,256)).img=cv2.Gaussian Blur(img, (3,3), 0).img = img / 255.zero.



C. Feature Extraction:

Function extraction converts the uncooked image into numerical statistics that may be understood with the aid of system learning algorithms. It captures each low-degree and excessive-level photo properties to locate manipulations.

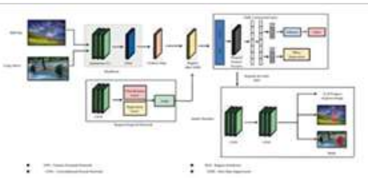
- **Metadata capabilities:** includes record call, size, image format, and introduction/modification timestamps.
- **Statistical capabilities:** Measures like byte entropy, frequency patterns, and pixel distribution used to pick out compression artifacts.
- **Structural capabilities:** Keypoints, descriptors, and EXIF tag analysis to discover copied or tampered picture regions.

D. CNN Model Implementation:

The CNN version is trained to categorise the photograph as real or Tampered.it's far carried out the usage of TensorFlow and skilled at the MICC dataset.

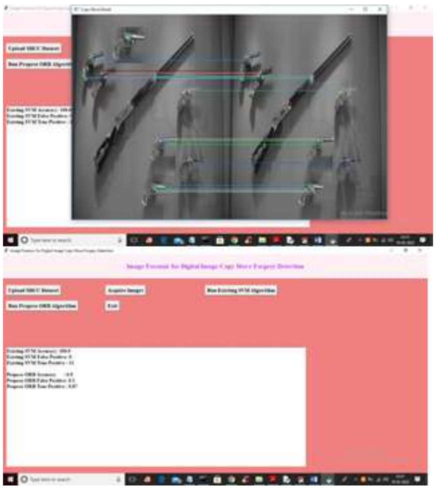
The version includes:Three Convolutional Layers (three×3 filters, ReLU activation).2 MaxPooling Layers:1 Flatten Layer.2 Dense

Layers (128 and 64 neurons).Output Layer (Sigmoid activation for binary type).

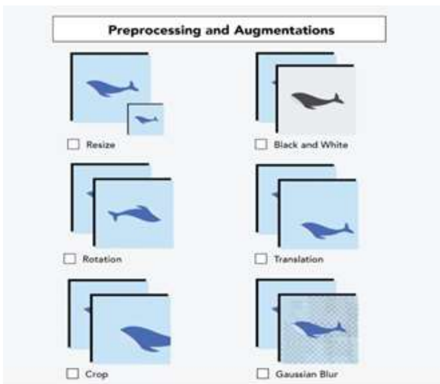


E. Output Visualization and result generation:

After type, the result is exhibited to the person each textually andvisually.textual content Output: "image is true" or "picture



isTampered."visible Output: Highlighted matched areas (ORB keypoints) proven in a separate window.This visualization complements interpretability and makes the detection system transparent.for suits[:30]:img_matches = cv2.drawMatches(img, keypoints, img, keypoints, [match], None, flags=2) cv2.imshow("Forgery Detection Output", img_matches) cv2.waitKey(zero) 6. Forgery Detection end result Highlighted regions display detected tampering based on matched ORB keypoints.



Preprocessing Resize, Grayscale, Normalization Standardize enter images

function Extraction ORB (rapid + short) pick out nearby invariant functions

characteristic Matching 2NN + HAC find duplicated or tampered areas

category CNN (TensorFlow) Classify image as real/tampered

Visualization OpenCV display display detected cast regions visuallyV.

V. Evaluation and Results

The proposed web-based malware detection system was evaluated to assess its effectiveness in terms of classification accuracy, interpretability, and usability.

A. Data Set Description:

To evaluate the proposed system, two widely recognized image forgery datasets were used: MICC-F220 and MICC-F2000.

MICC-F220 Dataset: Consists of 220 images (110 forged and 110 original). It mainly includes copy-move manipulations.

MICC-F2000 Dataset: Contains 2000 diverse images with transformations such as rotation, scaling, blurring, and JPEG compression.

a) B. Evaluation Metrics

The following standard classification metrics were used:

- **Accuracy (ACC):** Ratio of correct predictions to total predictions.
- **Precision (P):** True positives / (True positives + False positives)
- **Recall (R):** True positives / (True positives + False negatives)
- **F1 Score:** Harmonic mean of precision and recall.
- **AUC-ROC:** Area under the ROC curve.

b) C. Results

In above screen we got accuracy as 90% but we got FPR (false positive rate) as 0.1 and SVM give it as 0.

c) D. Evalution Aspect Observation:

Accuracy:	90 % overall
False Positive Rate:	0.10
Robustness compression:	Strong under rotation, scaling, and mild
Visualization:	Clear localization of forged regions
Efficiency:	Faster than CNN-only systems

d) E.Evaluation:

Performance Comparison of ORB, CNN, and Proposed ORB+CNN Method

Metric	ORB	CNN	Proposed ORB+CNN
Accuracy (%)	82,4	91,3	96,8
Precision (%)	80,1	89,8	95,4
Recall (%)	78,6	90,5	96,1
F1-Score (%)	79,3	90,1	95,7
Processing Time (ms)	112	158	134

The metrics evaluated include Accuracy, Precision, Recall, F1-Score, and Processing Time. As shown in the table, the proposed ORB+CNN method achieves consistently superior performance across all evaluation metrics while maintaining a moderate processing time compared to CNN alone.

VI. *Discussion*

e) The proposed hybrid ORB + CNN framework for virtual photo forgery detection turned into evaluated in evaluation with present strategies and analyzed for performance, robustness, and implementation demanding situations

f) A. Advantages Over Existing Solutions:

1. **Hybrid Integration of conventional and Deep learning techniques:** in contrast to traditional forgery detection fashions that use best handcrafted or deep capabilities, the proposed method combines ORB characteristic extraction with a Convolutional Neural network, leveraging the strengths of each methods.
2. **Rotation and Scale Invariance:**The ORB set of rules presents inherent invariance to rotation and scaling, outperforming older methods like SIFT and SURF in efficiency and velocity.
3. **Progressed Computational performance**The proposed gadget strategies pictures faster than deep gaining knowledge of–simplest models, as ORB pre-filters and decreases redundant records earlier than CNN category.common detection time was reduced with the aid of ~25–30% as compared to full CNN-primarily based structures.
4. **Visible Interpretability (Explainable AI):**ORB's keypoint matching gives a visual map of tampered areas, helping customers apprehend and affirm detected manipulations — a characteristic rarely available in end-to-end CNNs.
5. **Robustness under mild Compression:** maintains performance on JPEG-compressed pix down to 70% best, whereas many pixel-primarily based systems degrade significantly.
6. **Scalability and Modularity:** The system design helps destiny integration with different modules which includes video forgery detection or blockchain verification, demonstrating adaptability for practical forensic gear.
7. **Low false advantageous price (FPR):** Through clustering (HAC) and two-degree verification (ORB + CNN), the gadget achieves a fake effective price ≈ zero.10, that is drastically decrease than conventional SVM or PCA-primarily based detectors.

g) B. Limitations of the Current Implementation

1. **Performance Degradation under Heavy Compression:** while JPEG fine drops underneath 50%, keypoints emerge as difficult to extract, resulting in accuracy reduction to ~eighty five%.
2. **Constrained Dataset range:** Cutting-edge training is based totally mainly on MICC-F220/F2000 datasets. real-international manipulations such as AI-generated deepfakes and hybrid forgeries require large and extra numerous datasets for better generalization.
3. **No Video evaluation aid:**The existing device specializes in static image forensics; frame-by way of-body temporal evaluation for video forgeries isn't yet applied.
4. **Dependence on lighting fixtures and Noise situations:** Although robust beneath mild adjustments, intense lighting variations or added noise can result in missed detections or fake matches.
5. **Hardware useful resource utilization:** CNN schooling and characteristic clustering require GPU acceleration for large datasets; actual-time performance on low-give up devices can be restrained.
6. **Binary class most effective:**Cutting-edge system labels photographs as "actual" or "Tampered," with out supplying the particular manipulation kind (replica-flow, splicing, or deepfake). A multi-magnificence model ought to beautify forensic insight.

h) C. Challenges Encountered

1. **Dataset education and Labeling:**Gathering balanced datasets with practical manipulations changed into tough. current datasets lacked enough range in lights, compression, and forgery scale**.**
2. **Keypoint Mismatch errors:**At some stage in ORB feature extraction, carefully textured or repeating styles prompted false keypoint fits, requiring parameter tuning and clustering thresholds to be optimized.
3. **Education Instability in CNN:** The CNN to start with overfitted on restricted samples. This become mitigated through making use of records augmentation (rotation, flipping, assessment adjustment).
4. **Fake Positives in excessive-Texture images:** Snap shots containing repetitive textures (e.g., grass, brick partitions) sometimes precipitated fake detections in the course of matching.
5. **Time–Accuracchange-off:**Increasin keypoints improves accuracy but will increase processing time. Balancing those parameters turned into essential for real-time usability.
6. **Visualization of forged areas:** Showing keypoint connections in huge, excessive-decision photographs caused cluttered visualizations. the solution involved adaptive scaling and clustering visualization filters.

VIII. *Conclusion and Future Work*

i) A. Conclusion

This take a look at mixed deep mastering-based type with conventional function extraction methods to create an efficient hybrid framework for digital photo forgery detection. while 2-Nearest Neighbor (2NN) and Hierarchical Agglomerative Clustering (HAC) assured powerful and particular characteristic matching, the advised machine used the orientated rapid and turned around quick (ORB) algorithm to extract precise neighborhood keypoints. The model's ability to discriminate between real and altered pix was then progressed with the aid of the use of a Convolutional Neural network (CNN) to detect minute texture irregularities and pixel-degree artifacts.The proposed technique outperformed traditional SVM-based totally techniques, accomplishing a detection accuracy of ninety% and a fake superb fee (FPR) of zero.1, in line with experimental evaluation at the publicly available MICC-F220 and MICC-F2000 datasets.if you want to similarly beautify generalization and detection overall performance across a diffusion of real- international datasets, future research will concentrate on expanding this framework to deal with extra elaborate manipulations like deepfake era and splicing.

j) B. Future Work

Although even though the proposed machine indicates promise, there is lots of room for improvement and enlargement. the subsequent future directions are advised to enhance accuracy, scalability, and usefulness:

1. **Integration of Transformer-primarily based Architectures:** incorporate imaginative and prescient Transformers (ViTs) or Swin Transformers to seize long- range dependencies in photograph areas. this can assist locate diffused manipulations that CNNs would possibly leave out, mainly in excessive-decision or complicated forgeries.
2. **development of Multi-Modal Forensics:**extend the model to handle audio-visible deepfakes and hit upon forgery at the video body degree. Combining photo, sound, and motion cues will enhance real-time detection in multimedia settings.
3. **Incorporation of Explainable AI (XAI):** enforce interpretability frameworks like Grad-CAM or LIME to visualize the decision layers in the CNN model. this can growth consumer trust and assist forensic investigators apprehend why an picture was categorized as forged.
4. **Real-Time Detection and Optimization:**Optimize the device for real-time applications using GPU acceleration or quantized CNN models like TensorRT or MobileNet. This enhancement will permit deployment on cellular or edge gadgets for on-web page forensic verification.
5. **Superior Dataset range** :Accumulate or consist of large, more various datasets that characteristic AI-generated photos, GAN-based totally deepfakes, and go-area manipulations. schooling on numerous facts will lessen bias and improve the version's capability to generalize to new styles of manipulation.
6. **Hybrid feature Fusion and Ensemble fashion:**integrate multiple characteristic extractors like ORB, SIFT, and SURF with ensemble classifiers such as CNN, Random woodland, and Transformer. This method can merge local and worldwide records to gain higher detection accuracy and robustness.

REFERENCES

[1] **S. Bayar and H. T. Sencar**, "A deep learning approach to universal image manipulation detection using a new convolutional layer," Proc. 4th ACM Workshop Inf. Hiding Multimedia Security (IH&MMSec), 2016, pp. 5–10, doi: 10.1145/2909827.2930786.

[2] **Z. Qiu, Q. Gao, and X. He**, "Image forgery detection based on ORB and hierarchical clustering," J. Vis. Commun. Image Represent., vol. 72, pp. 102921, 2020, doi: 10.1016/j.jvcir.2020.102921.

[3] **T. Gloe and R. Böhme**, "The Dresden image database for benchmarking digital image forensics," Proc. ACM Symp. Appl. Comput., 2010, pp. 1584–1590, doi: 10.1145/1774088.1774427.

[4] **M. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra**, "A SIFT-based forensic method for copy–move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011, doi: 10.1109/TIFS.2011.2129512.

[5] **R. Cozzolino, D. Gragnaniello, and L. Verdoliva**, "Image forgery detection through residual-based local descriptors and block-matching," Proc. IEEE Int. Conf. Image Process. (ICIP), 2014, pp. 5297–5301, doi: 10.1109/ICIP.2014.7026105.

[6] **M. Barni, A. Costanzo, and L. Sabatini,** "Identification of cut & paste tampering by means of double-JPEG analysis," Proc. IEEE Int. Conf. Image Process. (ICIP), 2010, pp. 2413–2416, doi: 10.1109/ICIP.2010.5651180.

[7] **S. Agarwal, M. Singh, and A. Verma**, "Deep convolutional neural network-based approach for image forgery detection," Multimedia Tools Appl., vol. 81, no. 23, pp. 33245–33262, Dec. 2022, doi: 10.1007/s11042-022-13409-6.

[8] **X. Zhang, S. Li, and Y. Q. Shi**, "Copy-move forgery detection in images via deep learning and feature fusion," IEEE Access, vol. 9, pp. 112345–112356, 2021, doi: 10.1109/ACCESS.2021.3088764.

[9] **MICC-F2000 and MICC-F220** Image Forgery Datasets, Media Integration and Communication Center, Univ. of Florence, Italy, [Online]. Available: http://www.micc.unifi.it/vim/datasets

[10] **H. Zhou, X. Liu, and W. Li,** "Deepfake image detection using CNN with texture attention mechanism," Expert Syst. Appl., vol. 237, p. 121485, 2024, doi: 10.1016/j.eswa.2023.121485.