**IEEE BASE PAPER TITLE:**

**Enhancing Digital Image Forgery Detection Using Transfer Learning**

**(or)**

**OUR PROPOSED PROJECT TITLE:**

**Digital Image Forgery Detection Using Deep Learning**

**IEEE BASE PAPER ABSTRACT:**

Nowadays, digital images are a main source of shared information in social media. Meanwhile, malicious software can forge such images for fake information. So, it’s crucial to identify these forgeries. This problem was tackled in the literature by various digital image forgery detection techniques. But most of these techniques are tied to detecting only one type of forgery, such as image splicing or copy-move that is not applied in real life. This paper proposes an approach, to enhance digital image forgery detection using deep learning techniques via transfer learning to uncover two types of image forgery at the same time, The proposed technique relies on discovering the compressed quality of the forged area, which normally differs from the compressed quality of the rest of the image. A deep learning-based model is proposed to detect forgery in digital images, by calculating the difference between the original image and its compressed version, to produce a featured image as an input to the pre-trained model to train the model after removing its classifier and adding a new fine-tuned classifier. A comparison between eight different pre-trained models adapted for binary classification is done. The experimental results show that applying the technique using the adapted eight different pre-trained models outperforms the state-of-the-art methods after comparing it with the resulting evaluation metrics, charts, and graphs. Moreover, the results show that using the technique with the pre-trained model MobileNetV2 has the highest detection accuracy rate (around 95%) with fewer training parameters, leading to faster training time.

**OUR PROPSOED PROJECT ABSTRACT:**

The advent of digital image manipulation tools has exacerbated the proliferation of image forgeries, necessitating robust solutions for their detection. This project presents a novel approach to address this challenge, utilizing Python and Convolutional Neural Network (CNN) model architecture. The CNN model, employed as the core of our forgery detection system, has exhibited remarkable performance. With a training accuracy of 98% and a validation accuracy of 92%, it showcases its efficacy in distinguishing authentic from tampered images. The dataset utilized in this study comprises 12,615 images, consisting of 7,492 authentic (real) images and 5,123 tampered (fake) images, providing a diverse and extensive testbed for evaluation. To enhance the precision of our approach, we incorporate Error Level Analysis (ELA) as a preprocessing step. Each image is resized to a standardized 256x256 resolution, after which ELA is applied. ELA aids in the identification of regions within an image that exhibit varying compression levels. In an untampered image, all regions should exhibit uniform compression. Deviations from this uniformity may indicate digital manipulation. The processed images are stored as numpy arrays for subsequent analysis. Our proposed system leverages the synergy between deep learning through CNNs and the subtleties uncovered by ELA. This combination empowers the model to not only achieve high accuracy but also to provide insights into the specific regions of potential manipulation within an image. By harnessing the capabilities of Python and a well-structured CNN architecture, this project represents a significant stride towards robust digital image forgery detection, with potential applications in various domains where image authenticity is paramount.

**EXISTING SYSTEM:**

* In the realm of digital image forgery detection, the utilization of deep learning techniques has become increasingly prevalent. An existing system, which employed the MobileNetV2 architecture, stands as a testament to the efficacy of this approach in addressing the critical challenge of detecting image forgeries.
* MobileNetV2 is a state-of-the-art neural network architecture that has been specifically designed for mobile and embedded vision applications. Its lightweight design and computational efficiency make it an attractive choice for tasks where resource constraints are a concern. In the context of digital image forgery detection, MobileNetV2 provides a streamlined and effective solution.
* The existing system, utilizing MobileNetV2, demonstrated impressive results in distinguishing between authentic and tampered images. Through a process of feature extraction and hierarchical learning, the model was able to capture intricate patterns and nuances within the images, thereby achieving high accuracy in forgery detection.
* One of the notable advantages of MobileNetV2 is its ability to strike a balance between model complexity and performance. It achieves this by employing depth-wise separable convolutions, reducing the computational burden while preserving the model's ability to learn intricate features. This efficiency is of paramount importance in real-time applications and resource-constrained environments.
* The existing system incorporated a diverse dataset, encompassing a wide array of authentic and tampered images, to thoroughly evaluate the model's performance. The MobileNetV2 architecture, combined with a well-curated dataset and appropriate training strategies, yielded a robust forgery detection system.
* Overall, the existing system's utilization of MobileNetV2 as its core architecture highlighted the adaptability and effectiveness of deep learning techniques in addressing the intricate task of digital image forgery detection. By harnessing the capabilities of MobileNetV2, this system paved the way for subsequent advancements in the field, setting a high standard for accuracy and efficiency in forgery detection applications.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Limited to Specific Use Cases: MobileNetV2, while efficient and lightweight, may not be suitable for all forgery detection scenarios. Its architecture is optimized for mobile and embedded vision applications, which means it may not perform as well as more complex models in tasks requiring a deep understanding of fine-grained image details.
* Reduced Accuracy on Complex Manipulations: MobileNetV2's simplicity can be a disadvantage when dealing with highly complex image manipulations. It may struggle to detect subtle and sophisticated forgery techniques that require a deeper understanding of image content.
* Resource Intensive During Training: Although MobileNetV2 is designed to be computationally efficient during inference, training such networks can still be resource-intensive. Training on large datasets with MobileNetV2 may require significant computational power and time.
* Limited Contextual Understanding: MobileNetV2 operates on fixed-size input images and may lack the ability to capture extensive contextual information. This can be a limitation when detecting forgeries that rely on the broader context of an image, such as inconsistencies in lighting, shadows, or reflections.
* Dependency on Dataset Quality: Like any deep learning-based system, the performance of MobileNetV2 is highly dependent on the quality and diversity of the dataset used for training. If the training dataset is not representative of real-world forgery scenarios, the model may struggle to generalize to new, unseen manipulations.
* Difficulty in Interpretability: Deep learning models like MobileNetV2 are often considered "black-boxes" in that it can be challenging to interpret why a particular decision was made. This can be a significant disadvantage when trying to understand and explain the model's behavior, which is crucial in forensic applications.
* Updates and Maintenance: Keeping the model up-to-date with emerging forgery techniques and adapting it to evolving threats can be challenging. Continuous monitoring and retraining may be required to maintain high detection accuracy.
* Resource Constraints: While MobileNetV2 is relatively resource-efficient, it may still be too demanding for deployment on resource-constrained devices or platforms, limiting its applicability in certain environments.
* False Positives/Negatives: Like any forgery detection system, MobileNetV2 may produce false positives (incorrectly flagging authentic images as forgeries) or false negatives (failing to detect certain types of forgeries). Balancing these errors can be a complex challenge.
* In summary, while MobileNetV2 offers many advantages in terms of efficiency and performance for forgery detection, it is not without its limitations. Its suitability depends on the specific use case, the complexity of the manipulations being detected, and the available computational resources for training and deployment. Careful consideration and potentially combining it with other techniques may be necessary to address these limitations effectively.

**PROPOSED SYSTEM:**

* The proposed system for digital image forgery detection is a comprehensive approach that combines Convolutional Neural Network (CNN) architecture with Error Level Analysis (ELA) to achieve accurate and robust detection of manipulated images. This system addresses the critical need for reliable forgery detection in the era of digital image manipulation.
* The proposed system employs a CNN model as its core. The CNN is designed to perform feature extraction and classification of images efficiently. The model is trained on a diverse dataset comprising both authentic and tampered images. During training, it learns to identify distinctive patterns, features, and inconsistencies that indicate image manipulation. Various hyperparameters, such as the number of layers, filter sizes, and learning rates, are fine-tuned to optimize the model's performance. Appropriate activation functions, such as ReLU (Rectified Linear Unit), are used to introduce non-linearity into the model.
* Before feeding images into the CNN, they undergo preprocessing using ELA. All images are resized to a standardized resolution (e.g., 256x256 pixels) to ensure consistency. ELA is applied to each image. This involves saving the image at a specific compression level and then subtracting this compressed image from the original image. The resulting ELA image highlights areas with differing compression levels, potentially indicating regions of manipulation.
* The proposed system utilizes a comprehensive dataset consisting of 12,615 images. This dataset is carefully curated to include a balanced mix of authentic and tampered images. There are 7,492 authentic (real) images in the dataset, representing a wide range of real-world scenarios. The dataset contains 5,123 tampered (fake) images, encompassing various types of digital manipulations commonly encountered in image forgery.
* After ELA preprocessing, the CNN model is used to classify each image as either authentic or tampered. The model's output provides a confidence score or probability indicating the likelihood of an image being tampered. A predefined threshold is applied to these scores to make the final binary classification decision.
* The proposed system is designed with the potential for real-time implementation, allowing it to be integrated into various applications and systems where instantaneous forgery detection is required. The system's performance is rigorously evaluated using standard metrics such as accuracy, precision, recall, and F1-score.
* In summary, the proposed system leverages the power of CNNs and ELA to create a robust digital image forgery detection solution. It offers a comprehensive approach to identifying manipulated images, ensuring the integrity and authenticity of digital visual content.

**ADVANTAGES OF PROPOSED SYSTEM:**

* High Accuracy: The proposed system combines the strengths of CNNs and ELA to achieve high accuracy in detecting digital image forgeries. The CNN's ability to learn intricate patterns and features is complemented by ELA's capability to highlight inconsistencies, resulting in precise detection.
* Robustness: By integrating ELA as a preprocessing step, the system gains robustness against various forgery techniques and manipulation types. It can effectively detect both simple and complex forgeries, making it versatile and reliable.
* Adaptability: The system's CNN architecture is highly adaptable and can be fine-tuned to specific forgery detection tasks. This adaptability allows it to perform well across a wide range of image content and manipulation methods.
* Diverse Dataset Utilization: The utilization of a comprehensive dataset comprising both authentic and tampered images enhances the system's ability to generalize. It has been trained on a wide variety of scenarios, ensuring it can handle real-world forgery challenges effectively.
* Real-Time Detection: The proposed system is designed with real-time implementation in mind, making it suitable for applications where immediate forgery detection is crucial, such as social media content filtering and forensic analysis.
* Interpretability: While deep learning models are often considered complex, the system's integration of ELA can provide some interpretability. It can highlight regions of interest in tampered images, aiding forensic analysts in understanding the manipulation.
* Scalability: The system can be scaled to handle large datasets and can take advantage of increased computational resources for improved performance. This scalability is valuable for applications that involve processing a substantial volume of images.
* Preventative Measures: Beyond detection, the system can also serve as a deterrent against digital image forgery. Knowing that robust forgery detection is in place can discourage potential manipulators, promoting image authenticity.
* Versatility: The proposed system's versatility extends to different types of digital media, including images with various resolutions and formats. It can be applied to both static images and video frames, expanding its utility.
* Continuous Improvement: As new forgery techniques emerge, the system can be updated and retrained to stay effective. This adaptability ensures that it remains a valuable tool for long-term image authenticity verification.
* Cross-Platform Integration: The system's real-time capabilities and adaptability make it suitable for integration into a wide range of platforms and applications, including social media platforms, digital forensics tools, and image editing software.
* In conclusion, the proposed system offers a robust and adaptable solution for digital image forgery detection, with numerous advantages that make it a valuable tool in preserving the integrity and authenticity of digital visual content.

**SYSTEM ARCHITECTURE:**

Predicted Results: Authentic (Real) Image (or) Tampered (Fake) Image

CASIA2

Image Dataset

CNN Model Architecture.

Performance Analysis and Graph

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium i3 Processor.
* Hard Disk : 500 GB.
* Monitor : 15’’ LED.
* Input Devices : Keyboard, Mouse.
* Ram : 8 GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 10 Pro.
* Coding Language : Python 3.10.9.
* Web Framework : Flask.
* Frontend : HTML, CSS, JavaScript.

**REFERENCE:**

ASHGAN H. KHALIL, ATEF Z. GHALWASH, HALA ABDEL-GALIL ELSAYED, GOUDA I. SALAMA, AND HAITHAM A. GHALWASH, “Enhancing Digital Image Forgery Detection Using Transfer Learning”, IEEE Access ( Volume: 11), 2023.