

A Deep Reconstruction-Based Scalable Framework for Image Forgery Detection

B Pavani¹, E Pranav Kumar², H Krishna Tejaswi³, J Siddartha⁴, K Shiva⁵, P. Navya⁶, Dr. S Shiva Prasad⁷

^{1,2,3,4,5}*Student, Department of CSE Data Science*

^{6,7}*Professor, Department of CSE Data Science*

^{1,2,3,4,5,6,7}*Malla Reddy Engineering college, Secunderabad*

Abstract—Currently, manipulation of digital images with modern powerful image editing software is a commonplace approach. Therefore, determining the authenticity of the image is one of the crucial challenges faced by multimedia forensics. The presented project incorporates RIFD-Net, a deep-learning-based system for detecting and localizing forged regions in images. At the heart of the system is an encoder-decoder network, inspired by U-Net architecture, performing pixel-level analysis to generate forgery masks visually highlighting tampered areas. In addition to the deep learning-based detection of forgeries, this system provides a REST API to enable real-time forgery confidence estimation that allows seamless connection with external applications and large-scale image databases. An EXIF metadata analysis module has also been included, which could identify missing or suspicious metadata patterns of images, hinting at tampering. Perceptual hashing for efficient detection of duplicate and near-duplicate images is conducted. The proposed model is first trained on paired original images along with ground-truth masks and optimized by using the Adam optimizer with mean squared error loss. A web interface using Streamlit will be presented that will enable real-time image uploading, analysis, and visualization. Experimental results establish that the system will be able to combine the complementary visual, metadata, and structural cues through effective processing, making it practical and scalable for modern digital image forensics.

Index Terms—Deep Learning, EXIF Analysis, Forgery Mask, Image Forgery, Image Splicing, Noise Detection, Perceptual Hashing, U-Net Architecture.

I. INTRODUCTION

Digital images have evolved to become one of the most crucial conveyors of information, evidence, or communication in several fields of life such as journalism, social media, judicial and police

investigations, and cybersecurity. The ubiquity of powerful image editing tools has made the task of manipulating digital images without leaving traces relatively easy. Images can undergo some important content changes via splicing, copy-move operations, and noise manipulations, and yet they will appear original to the naked eye. Ensuring the authenticity and integrity of digital images has, therefore, become one of the prime tasks in the area of multimedia forensics.

Conventional approaches to image forgery detection rely on handcrafted features, statistical measures, or heuristic-based methods. Although such methods can indicate the presence of specific types of manipulations, their generalization to a wide range of forgery techniques and real-world image conditions is poor. Furthermore, most of the traditional systems are designed to classify images as forged or authentic without revealing the exact location of manipulation. The absence of localization decreases the interpretability and forensic value of the applied detection process.

With the aim of surmounting these limitations, this project introduces a Deep Reconstruction-Based Framework for Image Forgery Detection, employing deep learning for detection and localization of image forgeries. The proposed system utilizes a convolutional encoder-decoder architecture inspired from the U-Net model, which is designed for pixel-level analysis of input images. The framework learns to reconstruct forgery-related patterns, generating a forgery mask that highlights manipulated regions, thus aiding in precise localization and interpretation of tampered areas visually. The encoder captures the high-level semantic features relative to forgery

artifacts, while the decoder reconstructs spatial details required for accurate region-wise detection.

Besides deep learning-based localization, the framework embeds other forensic modules that allow increasing the detection reliability: EXIF metadata analysis allows for the detection of missing or inconsistent metadata that could suggest tampering with an image; perceptual hashing allows fast detection of duplicate and near-duplicate images. In such a way, the system could be integrated with external applications and large-scale image databases to offer real-time REST APIs for automated forgery analysis. A Streamlit-based web interface wraps the code in an interactive, user-friendly environment, allowing users to upload the images and analyze them, while showing the results in a readable format. Overall, the proposed framework follows a judicious combination of deep reconstruction learning, metadata inspection, and system-level deployment to deliver a pragmatically effective, scalable, and interpretable solution for modern digital image forgery detection.

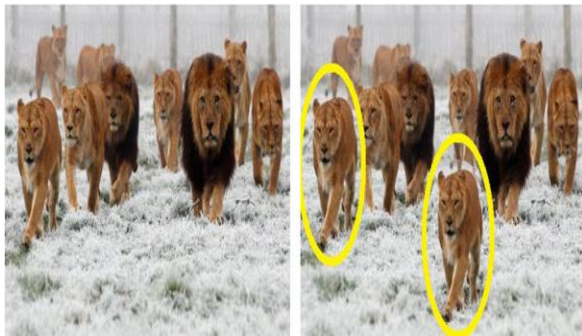


Figure.1 Illustration of Forgery

II. LITERATURE SURVEY

Digital image forgery detection has emerged as a recent highlight in the domain of multimedia forensics, considering both the rapid growth of manipulating tools and their malicious usage. Early attempts in this realm relied more on traditional image processing and some statistical analysis techniques. Those techniques took issues with inconsistencies in color distribution, edges, texture, and compression artefacts for the detection of manipulated images [1]. Such methods were bound to be effective only under highly constrained conditions and relied on handcrafted feature extraction. Furthermore, they also showed much sensitivity against variations caused by post-processing of images.

Copy-move forgery detection was among the first and most researched manipulation detection techniques. Several block-based methods using DCT and PCA were proposed to find duplicated regions in the same image. Key-point-based methods applied SIFT and SURF key points to enhance robustness against rotation and scaling. Still, these techniques were computation-intensive and usually failed when images were noised, compressed, or underwent complex transformations.

Image splicing detection methods have been proposed to identify forged images generated by combining regions from different images. Several methods have inspected inconsistencies in lighting conditions, color correlation, and camera sensor noise patterns to detect the splicing operations [4]. While these methods achieved performance improvement in detecting forgery, their efficiencies were still subject to careful forgeries and usually output image-level classification results without precise localization of tampered regions.

For overcoming the limitations of handcrafted feature-based methods, CNNs were introduced with the advancement of deep learning. The CNN-based methods outperformed others by learning the discriminative features automatically from the image data itself [5]. However, most of these early deep learning models focused on binary classification tasks, that is, classifying an image as forged or authentic, without providing any visual explanation or even a method to determine the location of manipulated areas.

U-Net-inspired encoder-decoder architectures were thus adapted for image forgery detection that enabled pixel-level localization. These works relied on reconstruction learning in order to retain spatial information and create forgery masks that highlight manipulated regions [6]. Reconstruction-based frameworks were thus successfully used to model subtle manipulation artifacts, including noise inconsistencies and structural distortions. Compared with the improved capability of localization, most works about deep learning for forgery detection were designed only based on visual features, without considering complementary forensic information.

Recent research has investigated metadata-based analysis as an added layer of verification to detect forgery. EXIF metadata have been analyzed for missing, inconsistent, or modified camera information

to detect tampering of images [7]. Similarly, perceptual hashing has been applied to the fast detection of duplicate and near-duplicate images by comparing fingerprints of visual similarities [8]. Although effective individually, these techniques are hardly integrated with deep learning-based forgery localization systems.

Most of the traditional approaches to forgery detection only consider offline or experimental settings, offering no real-time deployment and practical usability. They consequently lack API-based inference and user-friendly interfaces, so as not to be adopted in a real-world context, such as large-scale image databases or computer-assisted content verification systems. A clear research gap from the reviewed literature lies in developing a unified image forgery detection system scalable and interpretable that unites deep reconstruction-based localization with metadata analysis and perceptual hashing for real-time deployment. The proposed framework for image forgery detection based on deep reconstruction fills this gap by integrating pixel-level deep learning analysis, EXIF metadata check, duplicate image detection, and API-based real-time inference within one deployable system.

III. PROPOSED METHODOLOGY

The proposed approach is a deep reconstruction-based framework for image forgery detection, encircling supervised deep learning and structured dataset preparation and preprocessing. This framework should be able to achieve both forged region detection and localization at the pixel level and handle multiple kinds of forgery. The total system focuses mainly on two broader classes of manipulations: splicing-based forgery and noise-based forgery. In accomplishing this, both classes are handled with carefully constructed datasets that allow the model to learn both structural and statistical inconsistencies that are caused during image manipulation. Thus, dataset preparation is a prime component of the framework and bears an important role in achieving complete and realistic forgery detection.

3.1 Data Creation

In creating the dataset for the proposed system, publicly available image data was put into a format that can be applied to supervised learning. The

splicing-based forgery dataset is sourced from a publicly available Dropbox repository, which contains authentic images, spliced images, and corresponding ground-truth forgery masks. These masks clearly reveal the manipulated regions in each image, facilitating effective pixel-level supervision while training. The noise-based forgery dataset is sourced from a repository of salt-and-pepper noise images on Kaggle. This dataset provides the clean images and their noise-corrupted version used to learn the inconsistencies caused by the artificial insertion of noise.

The dataset is organized into two main categories of forgery. In splicing-based forgery, manipulated images are generated by splicing regions across different source images and exhibit faint discrepancies in boundaries and textures. Correspondingly, a binary mask is provided for each spliced image, in which manipulated pixels are marked against authentic regions. On the other hand, noise-based forgery adds artificial noise into images, altering statistical properties but without apparent changes to any major structures. There is no explicit binary mask used in the noise-based forgery; instead, clean and noisy image pairs are provided to enable the reconstruction-based learning of noise inconsistencies.

Binary masks utilized in the splicing dataset are generated by highlighting the exact regions concerned with manipulation in the course of splicing. The masks are stored as grayscale images and later converted into binary representations where forged regions are represented by white pixels and non-forged by black pixels. This kind of precise labeling helps the model to learn accurate forgery boundaries during its supervised training. All image data, including original images, forged images, masks, and noise pairs, should be systematically organized and converted into NumPy array format to support efficient loading and processing during model training.

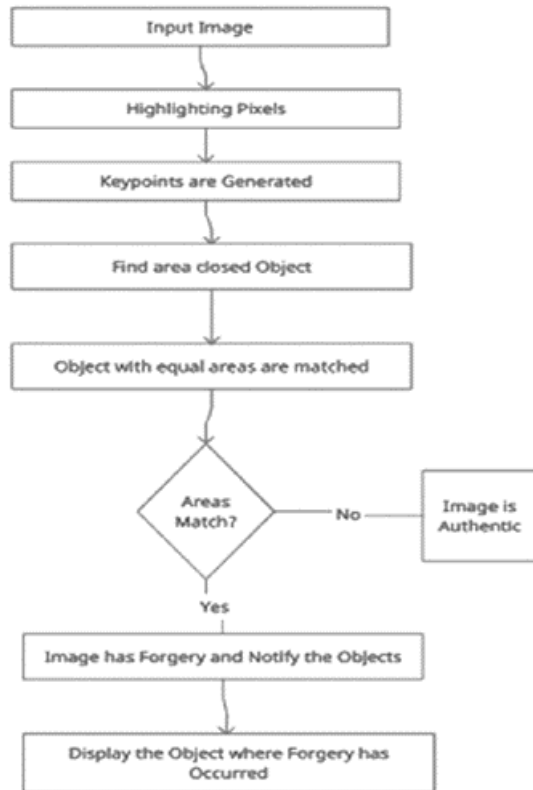


Figure 2. Forgery Detection Flow

3.2 Dataset Preprocessing

It is an important preliminary step in data preprocessing for uniformity, numerical stability, and compatibility of the dataset with the deep learning model. All images are converted into RGB format and then resized to a fixed resolution of 256×256 pixels to have a consistent resolution quality from different sources. The pixel values are normalized in the range of 0 to 1, which enhances the convergence during training and avoids numerical instability. These preprocessing steps ensure that the model receives standardized input regardless of the original image resolution or format.

For forgery detection based on splicing, binary masks go through the same resizing and normalization procedures as the original images. Each mask is spatially aligned with its corresponding image so that pixel-wise correspondence is guaranteed for training. This becomes crucial in correctly computing the loss and also accurately localizing the forged regions. These preprocessed image-mask pairs allow the model to effectively learn the reconstruction patterns associated with splicing artifacts. It basically pairs noisy images with their clean reference images. As a

result, the images are matched in size, normalized, and aligned for the reconstruction-based learning process. Such data would then undergo a random shuffle in order to minimize any learning bias, followed by a division into training and testing sets to evaluate its performance in terms of generalization. The above-mentioned steps belong to preprocessing through which the model gets learned about noise inconsistencies that hint at tampering. Overall, the creation and preprocessing of the dataset ensure that the proposed deep reconstruction-based framework is trained on good quality and well-structured data. Such systematic preparation of splicing and noise-based forgery datasets enables effective learning of manipulation artifacts and largely contributes to the accuracy and reliability of the image forgery detection system.

3.3 PROPOSED METHODS

The proposed system introduces the Deep Reconstruction-Based Framework for Image Forgery Detection. The main purpose of the proposed approach is not only the detection of image manipulation but the identification of the forged regions as well. The proposed framework is capable of addressing multiple types of image manipulations, including splicing-based image forgery and noise-based image forgery, utilizing a unified reconstruction learning approach. The proposed approach involves a number of steps, including the preparation of the dataset, training of the deep learning model, location of the forgery, metadata analysis, verification of perceptual similarity, and deployment of the system using an interactive interface and API.

3.3.1. Deep Reconstruction-Based Forgery Detection Algorithm

The main algorithm applied within this project is a Convolutional Encoder-Decoder Network, which is a variant of the U-Net structure and is applied for reconstruction-based learning. Contrary to common classification architectures, this method is applied for pixel-wise prediction and is used for locating tampering areas. The encoding part of this neural network includes a number of convolutional layers followed by max pooling layers. These layers, gradually, extract higher semantic features like texture, edge, and noise irregularities introduced during tampering.

While the input image progresses through the encoder, the resolution is decreased, whereas the depth increases, which facilitates abstract feature learning for forgery details. The reconstruction phase, involving the decoder, recovers the resolution by utilizing up sampling layers. The reconstruction-based approach for learning facilitates the usage of abnormal patterns, as there is no need for feature engineering. The mask for forgery, which was previously designed manually, can now be obtained from the model.

The proposed model is trained with input image pairs and ground truth. In cases involving image splicing, as an example of forgery type, ground truth is in the form of a binary mask, with regions as either forged or non-forged. In cases involving forgery using noise, unlike previous approaches, this proposed approach trains an image reconstruction mechanism to restore clean versions of images using input images contaminated with noise, thereby addressing inconsistencies with respect to noise. The Adam optimizer has been utilized to enable optimal convergence. The mean squared error function has been utilized to ensure that predictions and ground truth match closely.

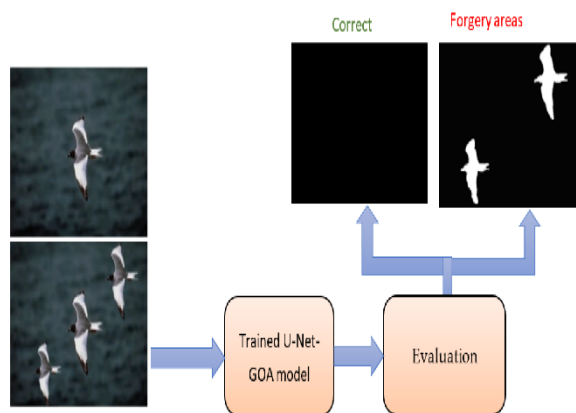


Figure 3. U-Net Model Forgery Evaluation

3.3.2 Splicing-Based Forgery

Splicing-based forgery detection involves assisting in finding areas in which image content has been merged from other images. Such forgeries bring in inconsistencies in boundary areas, textures, and noise. In this project, splicing forgery detection involves supervised learning in terms of pixels. In this process, every spliced image has been provided with a forgery image that distinguishes pixels within counterfeit areas from real image pixels.

Through training, the encoder-decoder network is able to link visual anomalies with regions that have been spliced in order to optimize the loss between the predicted and actual masks. The network output is hence the forgery mask that helps pinpoint the regions for forensic analysis. This method is more interpretable than binary classification.

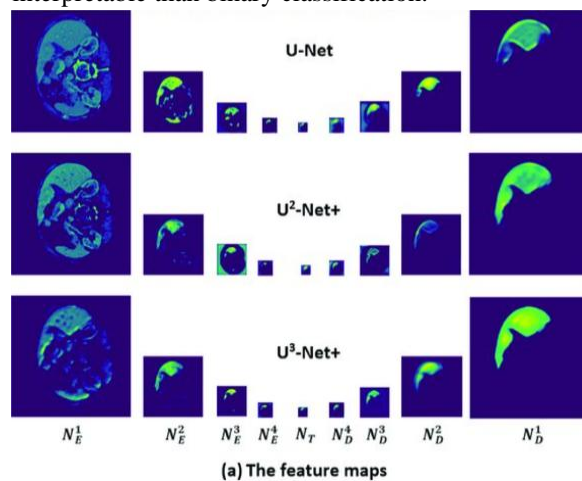


Figure 4. Working of U-Net Model

3.3.3 Noise-Based Forgery

This model for noise-based forgery focuses on the manipulations created by the insertion, filtration, or smoothing of artificial noise. This process can potentially lack the presence of apparent structural alterations but may vary the statistical characteristics of the image instead. In this scenario, the idea aims to address this issue by incorporating a learning process based on the reconstruction of both the clean image and the noise.

The model is trained on reconstructing clean images from noisy images. When reconstructing, discrepancies between the reconstructed image and the original image reveal possible tampering. This model allows for detection of noise level manipulation, which can be difficult to reveal by visual inspection. Noise level manipulation can add robustness to the framework since it tackles manipulation schemes that are not based on explicit region replacement.

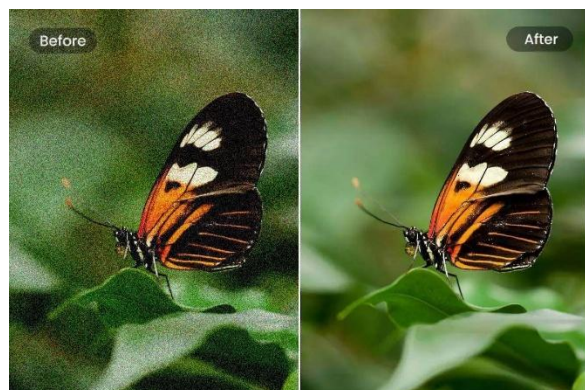


Figure 5. Denoising Noisy Image

3.3.4 EXIF Metadata Tampering Detection Algorithm
Apart from the visual analysis feature, the project combines the analysis of EXIF image metadata for the purpose of complementing the forensic analysis. The EXIF image metadata is typically comprised of details such as the model type, date taken, resolution, as well as the software used in the image processing. The project is capable of analyzing the available EXIF image metadata for inconsistencies.

Images lacking metadata, contradictory camera information, and traces of photo editing software are considered suspicious and potentially tampered. Although inconclusive metadata analysis cannot be used as proof of tampering, it is important subsidiary evidence that enhances the whole analysis process. This module enhances the analysis process and adds accuracy using both visual and non-visual forensic features.

3.3.5 Perceptual Hashing Algorithm of Similarity of Images

Perceptual hashing is applied to find duplicate and near-duplicate images effectively. Unlike traditional hash functions (cryptographic hashes), perceptual hashes produce hashes that are similar for images that look alike although possibly different in some way owing to compression or minor modifications. This project applies perceptual hashing to produce a hash of an image that is compared against existing hashes to find images that are reused or altered.

It is helpful in massive-scale forgery verification of images because it aids fast similarity searches. Perceptual hashing is useful in conjunction with deep learning-based forgery detection because it allows

analysis of structural similarity irrespective of pixel-wise learning.

3.3.6 Commercial and Customer Contacts

The FO of the system starts when an image is uploaded by a user either through the interface or through an API. The image will undergo pre-processing techniques like resizing, normalization, and format change. The pre-processed image will then go through a deep reconstruction-based forgery localization. At the same time, the EXIF metadata analysis and perceptual hashing process takes place. The results obtained from all the modules are combined to obtain the final result, which comprises the results for the confidence in the forgery, the result for the predicted forgery mask, the results for the metadata analysis, and the results for the similarity verification.

3.3.7 Key Features of Proposed System

This system allows for the localization of forgery at the pixel level as opposed to just classification, making it more interpretable and useful for forensics. It handles various types of forgery, including splicing and those involving noise, under this single model. EXIF analysis and perceptual hashing also make this system more robust at visualization-independent forensics as it entails both visualization and non-visualization forensics analysis. This system allows for real-time inference using API, thereby easily incorporating into other applications or large databases.

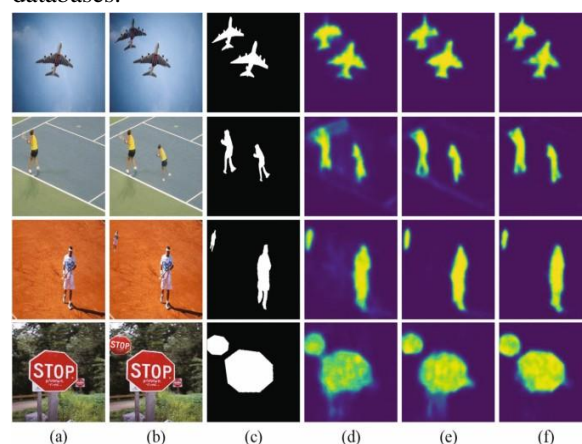


Figure 6. Prediction of Forgery Image using Binary and Heatmap Masks

IV. RESULTS

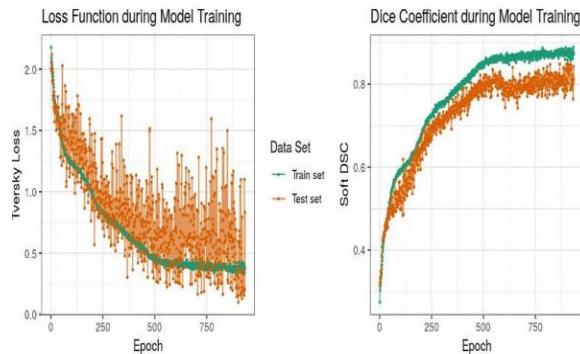


Figure 7. U-Net Model Evaluation Metrics

The proposed Deep Reconstruction-Based Framework for Image Forgery Detection was tested using a variety of image scenarios, including both real and fake areas of the image. The proposed framework is capable of detecting image forgery, identifying areas of image manipulation on a pixel-by-pixel basis, as well as examining inconsistencies of image metadata while producing accurate confidence scores by means of real-time processing. The proposed system is able to accomplish these tasks successfully.

In the context of forgery mask detection using splicing, the reconstruction model used in the proposed approach successfully identified the manipulated parts by providing a pixel-level mask of forgery. In different test scenarios, the predicted forgery masks were found to be very close to the actual masks, thus indicating the delineation of boundaries as well as the manipulated areas. The result showed successful reconstruction model performance, as the model efficiently picked the structural inconsistencies like texture, boundary, and light variations, usually observed in splicing, using the encoder-decoder approach.

However, in the context of noise-based forgery detection, the reconstruction learning algorithm helped the network to learn how to spot discrepancies resulting from noise insertion and filtering actions. The network learned to spot discrepancies in noise level manipulation that are usually imperceptible to human observation. This clearly showcases that despite lack of regional replacement manipulations in forgery methods, the proposed framework performs well.

Another aspect that aided the detection system is the analysis of the metadata of the images. Missing or inconsistent metadata in the EXIF has been identified in the test images using metadata analysis. It is important to note that the analysis of the metadata of the image alone cannot be used to detect image forging. However, the combination of the analysis of the metadata with the visualization of the forged image has been of great use. Images with missing metadata or trace amounts of editing software were also identified correctly.

The REST API ensured a steady flow of structured and interpretable results for each of the images tested. The outcomes of the forgery classification of images included the classification result together with the quantitative values of the forgery percentage and the confidence score. The forgery percentage gave information about the amount of manipulation in the image, while the confidence score indicated the model's certainty in the classification. High confidence scores were usually taken in cases of heavily forged images, while the scores were lower in cases of subtle images.

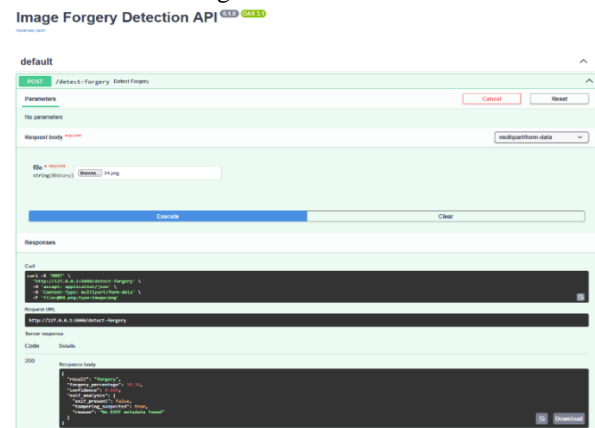


Figure 8. Forgery Detection API Test Results

The Streamlit interface enabled intuitive visualization of the results, allowing direct comparisons between the original images and the predicted forge masks. The proposed approach has become more interpretable due to the web interface and API layer, which ensures the stability and readiness to be implemented of the design. Consistent results from the web interface and API layer emphasize the readiness of the proposed approach to be implemented. In conclusion, the experimental evaluation proves that the deep reconstruction-based method introduced in this article

is indeed effective in detecting and locating image forgery in images with various types of forgery and image conditions. The integration of pixel-level deep learning analysis with metadata examination, perceptual similarity check, and real-time processing capabilities into this method has made it reliable, interpretable, and scalable in digital image forgery detection tasks.

✦ Metadata Analysis

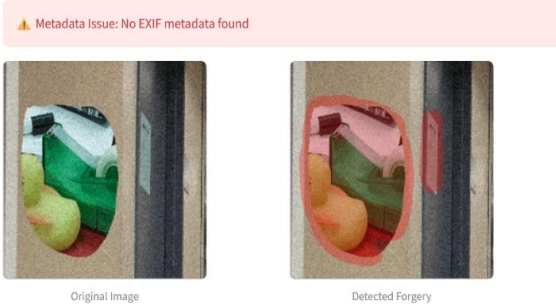


Figure 9. Forgery Detection using Forgery Mask

V. CONCLUSION

This work presents a Deep Reconstruction-Based Framework for Image Forgery Detection with a view to the growing challenge of image authenticity verification due to advanced digital manipulation techniques. Furthermore, the proposed system was designed to go beyond traditional methods in image-level classification with state-of-the-art performance in pixel-level forgery detection and localization to offer both accurate detection and clear visual interpretability. By leveraging a convolutional encoder-decoder architecture inspired from U-Net, the framework effectively learned structural and statistical inconsistencies introduced during image tampering.

The experimental evaluation showed that the reconstruction-based learning strategy is effective in finding forged regions within varied manipulation types, splicing-based and noise-based forgeries. This generating of forgery masks for precise localization of tampered areas enhanced forensic reliability significantly compared to the usual binary detection methods. Noise-based forgery analysis further improved robustness by rendering the system capable of detecting subtle statistical alterations-often very difficult to perceive with simple visual inspection.

Besides deep learning-based visual analysis, the combination of EXIF metadata inspection and perceptual hashing reinforced the general detection process by adding complementary forensic cues. Metadata analysis supplied supportive evidence in those cases where the detection based on a pure visual approach was insufficient, while perceptual hashing allowed the identification of near-duplicates and duplicates in an efficient manner. Combining the results of visual, metadata, and similarity-based analysis resulted in a more complete and trustworthy forgery detection framework.

This has been demonstrated in a proposed system through the implementation of a REST-based API and a Streamlit-powered user interface. Real-time inference, structured response outputs, and intuitive visualization capabilities make the framework suitable for integration with external applications, large-scale image repositories, and automated verification pipelines. The design at the system level guarantees that the proposed solution does not remain limited to experimental evaluation but is capable of solving digital forensics challenges in real-world scenarios. Overall, the proposed Deep Reconstruction-Based Framework for Image Forgery Detection effectively unifies deep learning, forensic analysis, and system deployment to form a single, scalable solution. It contributes to the field of digital image forensics, providing an interpretable, robust, and practical approach toward the detection and localization of image manipulations. The results from this work illustrate the potential of the reconstruction-based deep learning model further down the road toward trust, authenticity, and reliability in digital visual media.

REFERENCES

- [1] H. Farid, "Image Forgery Detection," IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, Mar. 2009.
- [2] J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images," Proceedings of the Digital Forensic Research Workshop, Cleveland, OH, USA, 2003.
- [3] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-Based Forensic Method for Copy-Move Attack Detection," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099–1110, Sept. 2011.

- [4] T. T. Ng, S. F. Chang, and Q. Sun, "Blind Detection of Photomontage Using Higher Order Statistics," IEEE International Symposium on Circuits and Systems, pp. 688–691, 2004.
- [5] B. Bayar and M. C. Stamm, "A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer," ACM Workshop on Information Hiding and Multimedia Security, pp. 5–10, 2016.
- [6] O. Ronneberger, P. Fischer, and T. Brox, "U-Net: Convolutional Networks for Biomedical Image Segmentation," Proceedings of the International Conference on Medical Image Computing and Computer-Assisted Intervention (MICCAI), pp. 234–241, 2015.
- [7] D. P. Kingma and J. Ba, "Adam: A Method for Stochastic Optimization," International Conference on Learning Representations (ICLR), 2015.
- [8] M. Kharrazi, H. T. Sencar, and N. Memon, "Blind Source Camera Identification," IEEE International Conference on Image Processing, vol. 1, pp. 709–712, 2004.
- [9] V. Monga and B. L. Evans, "Perceptual Image Hashing via Feature Points," IEEE Transactions on Image Processing, vol. 15, no. 11, pp. 3453–3466, Nov. 2006.
- [10] L. Verdoliva, "Media Forensics and DeepFakes: An Overview," IEEE Journal of Selected Topics in Signal Processing, vol. 14, no. 5, pp. 910–932, Aug. 2020.
- [11] A. Gulli and S. Pal, Deep Learning with Keras, Packt Publishing, 2017.
- [12] Streamlit Inc., "Streamlit: A Framework for Building Data Apps,". Available: <https://streamlit.io>
- [13] S. Ramírez et al., "Salt-and-Pepper Noise Removal in Digital Images," International Journal of Computer Applications, vol. 123, no. 3, pp. 1–6, 2015.
- [14] Kaggle, "Salt and Pepper Noise Images Dataset,". Available: <https://www.kaggle.com/datasets/rajneesh231/salt-and-pepper-noise-images>
- [15] Dropbox Public Dataset Repository, "Image Splicing Forgery Dataset,". Available: <https://www.dropbox.com/scl/fo/1stuwnt71fpxk7jjdyag>