International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Fake Image Forgery Detection

G PRAVEEN KUMAR, (Reg No: 231CT048)
UG Graduate, Department of Computer Technology,
Dr. N.G.P. Arts and Science College, Kalapatti road, Coimbatore, Tamil Nadu, India.
(Affiliated to Bharathiar University, Coimbatore)

Mrs.P VANITHA, Associate Professor, Department of Computer Technology,Dr. N.G.P. Arts and Science College, Kalapatti, Coimbatore, Tamil Nadu, India. (Affiliated to Bharathiar University, Coimbatore)

https://doi.org/10.55041/ijsmt.v2i3.22

Cite this Article: KUMAR, G. P. (2026). Fake Image Forgery Detection. International Journal of Science, Strategic Management and Technology, *02*(03). https://doi.org/10.55041/ijsmt.v2i3.223

Abstract

In the contemporary era, digital images are a vital source of information in the modern day, and as such, they are regularly disseminated on social media. False identification could be inferred from the deceptive information. With the many tools and methods that are available today, anyone can quickly create image forgeries that could pose a number of problems for society. Many of the strategies for identifying false identification have been explored in the literature survey that is currently available, but they are unable to provide an accurate result in real-world scenarios. Instead, they can only identify a single type of falsification in an image, such as cloning or resizing. This paper introduces an AI-driven image tampering identification system that will identify various forms of image manipulation.In order to detect forgeries, this study suggests a convolutional neural network-based model. The data will be collected as images and preprocessed by identifying any redundant information or missing values. The image yields several attributes, including dimensions, hue, length, breadth, and height. CNN receives all of the derived characteristics for training. The model uses the CMF technique to identify forgeries and then classifies the image as either forged or not. If an image is forged, it outputs the image containing the location of the faked image. The recommended method will reveal different images based on actual events and produce a 98% accuracy rate in counterfeit detection.

Keywords:CNN-Convolutional Neural Network, CMF-Copy-Move Forgery, ML-Machine Learning.

INTRODUCTION

Nowadays, Images and videos are spreading very vastly all over the world. Images plays major role across multiple domains such associal media, research, education, sports, forensics, medical, scientific etc. The images are used as among the main sources of information, so the image contains a specific information, by look into the image the user can easily understand the nature instead of the written words. There are numerous editing tools like photoshop, adobe, lightroom, Canva, Snapseed, pixel,paint shop etc. These tools perform tasks such as cropping image, resizing, colorcorrection,applying filters and effects. So, the imageforgery becomes easy and it is harder to detect. Detecting or identifying such forgeries is very crucial for maintaining the integrity.

Image forgery detection refers to the process of detecting isapicture has been manipulated or altered from its original state and also it focusingonidentifying andanalyzingmanipulated images. Image forgery has evolved significantly over the years by increasing theaccessibility of various image editing tools and techniques to convey users to false information. Nowadays various software is there to create image forgeries. By looking into the forged image user may get confused in detecting whether the image is tampered or not because forged image is very similar to original form. Sometimes the confused decision may

lead to false identification and it may cause some issues. To ensure the authentication of image, someMLand deep learningtechniques are employed in the proposed method.The main goal of picture authenticity verification using ML and deep learning approach is because these approaches detect the pinpoint modifications and alterations, manipulation in digital image easily. The traditional methods often rely only on hand crafted features and statistical analysis, which may hard or difficult to keep up with the large datasets and variety of modern forgeries. So, the modern technologies are used, neural networks models, particularly CNN (convolutional neural networks) are used to train large datasets containing both authentic and tampered images. Onusing these models, they detect various types of forgeries likesplicing, copy-move, inpainting and metadata manipulation. Advanced deep learning pattern recognition capabilities offers a more robust solution.

1. LITERATURE SURVEY

Dr. K. Prasanthi, Jasmine, S. K. Fhareedh, M. Navyan, K. Abhishek [1]. The project main goal is to recognize the forgery image, so it helps to ensure the authentication of pictures. To uncover the forged image, they have used Machine-Learning algorithms to pinpoint the manipulated image and configurations in data, by using these techniques we trained the data, so it is easy to identify the accurate trends in the picture and also, they have utilized Deep Learning techniques, such as deep neural model to identify the modified image. Dubey Krishna Pradeep, Gupta Sejal Kailash, Patil Viraj Kunjan, Mrs. Pallavi Patil [2]. This paper includes a unique approach to illustrate the fake image detection website using python. Now- days fake images is suitable for various purpose, so to avoid those frauds they create a website, they have utilized integrating state-ofart image analysis techniques to evaluate the picture and also, they have employed MachineLearning techniques. This website detects the fake image and also provides a user-friendly interface to upload the image and examine the photo accuracy.

Syed Sadaf Ali, et al., In this study they present a strong deep learning system to classify the image forgeries. The main difference between original image and recompressed image is the original are look like normal and real but recompressed images are highlighted which means forged parts gets highlighted, so it is easy to recognize the altered image. They used various methodologies to detect Splicing and Copy Move types of images.

Anushka Singh. Now-days the images and videos are spreading very fastly with the existence of editing tools, so this paper emphasizes on those scams, to detect the edited image they have used neural networkstrategies such as CNN. Later they used different transfer learning for pre-trained image through fine- tuning and implement those trainings to their data. They collect dataset as CASIA V2.0, by implementing the pre-processing techniques with some basic CNN model, later they done with 97% of accuracy with areal image. Amit D, Maitreyee Dutta, Gaurav K [5]. In this study the authors proposed an approach for detecting image forgeries. The paper contains dataset about 110 nonforged and 110forged images and the proportion of the image are in pixels. They have used Google Net approach to extract features of the images and later they implement techniques such as Random Forest algorithm to identify whether the photo is forged or not. It split the information within training and validating data and also match with state-of-the- approaches.

Siddesh Gaddadevara MATT [6]. This paper detects the image forgeries using fusion approach, which is lightweight model they employ diverse methods such as SqueezeNet, MobileNetV2, ShuffleNet. They pre-trained the model and achieves better accuracy as compare to the state-of-art approaches. Ashgan.H.Khalil etal.,[7]. This paper proposes a new technique to detect the image forgeries using transfer learning they adopt the binary classification and pre-trained the model by eight different

techniques which compares the result approximately 95%.

Sankalp Patekar etal.,[8]. This paper concludes forgery identification by CNN model, which have the ability to retrieve the essential features and the model analyze the Error Level and Noise Ratio to enhance the reliability and Emad UI Haq Qazi etal.,[10]. The paper uses most traditional, widely used approach for forgery detection, using CNN model it will collect the large dataset from BOW and reduced by utilizing pre-trained model. The technique is evaluated performance and achieved high ac- curacy.

[10]	Identifica- tion of manipulated image	CNN mod- el	BOW	CopyMove and Retouching

trustworthiness to the public. Preethi Sharma etal.,[9]. This paper gives general solution to the public, which involves active, passive and deep learning techniques to identify the forgeries and also data driven methods. Which will work effectively and deals with the intense forgeries in future also.

1.1 Table Comparison: -

Paper	**Aim**	**Tools and Methods used**	**Dataset**	**Types of Forgery**
[1]	Identifying image forgery	OpenCV and MD5	CASIA public dataset	Splicing and Copymove
[2]	Detecting a tampe red image	Google Net and an-dom Forest algorithm	MICC- F220, it consists of 220 images	Cloning and Copymove
[3]	Identify- ing fake images	Block matching and error level analysis	The input data can be given by t he user asimage	Resizing, Cloning and Splicing
[4]	Identify- ing the recompressed image	Deep learning algo- rithm	CASIA 2.0, i t contains 12614 images	Splicing and Copymove
[5]	Identify the tampered image	Deep Learning technique	General Images	Cloning and Splicing
[6]	Detecting forgeries using active ap- proach	Squeeze Net and Shuffle Net	K4	Copy- Move
[7]	Identify image forgeries	Using Transfer Learning	CASIA	Cloning and Overlay
[8]	Altered picture classification	CNN mod- el	General dataset	Retouching
[9]	Classifica- tion of Fake im- age	Error level analysis and Noise Ratio	K4	CopyMove and Cloning

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

3. OBJECTIVES

The goal of proposed method isspecified as follows: -

1. To design robust and accurate model for image integrity analysis.
2. To assess the precision of the model.

4. PROPOSED METHODOLOGY

The proposed methodcollects the various images and every image has to undergo the training process to understand the language, after the training process, CNN model detects the forged image. The entire process is represented in the Fig 4.1.

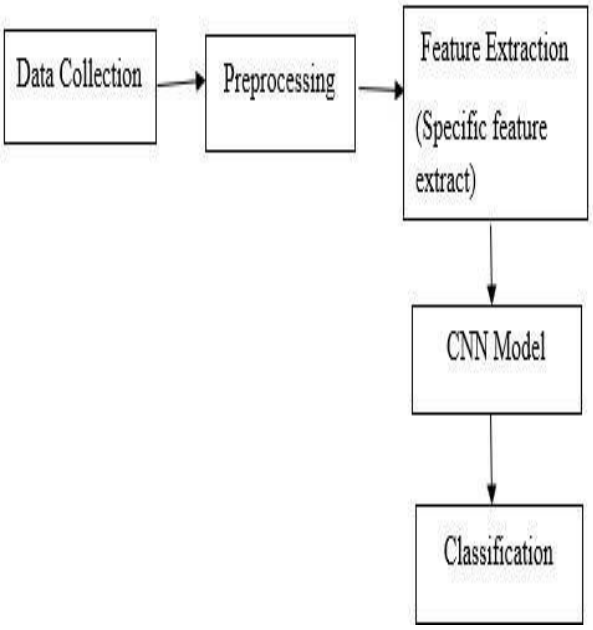

Fig 4.1: Proposed Flowchart of Forgery Detection

a) Data Collection :-

Data collection is the first process in the proposed method. Collecting various images for fraud detection which involves assembling of representative dataset, which includes various categories of image alteration and conditions.

Fig 4.2.a: Standard dataset

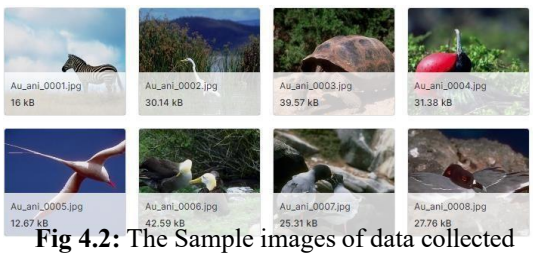

Fig 4.2: The Sample images of data collected

Fig 4.2.b: Manuallycollected dataset

In the above Fig 4.2 The image is collected manually as well from the standard dataset. Standard dataset consists of 800 images and manually 40 images are downloaded from the chrome, they consist of both forged and not forged images.

b) Preprocessing :-

The preprocessing, it serves as a context of deep learning. Which is employed to clean, transform, organize raw data before it is fed to training process. It usually gives the missing values, eliminating irrelevant or redundant information etc.

Data collected		Preprocessing steps	Description
		Space transformation	Changing the color space
		Resizing	Adjusting the image size to standard
		dimension	
	Normalization	Scaling pixel values to specific range [0,1]	
	Cropping	Removing unnecessary parts	

Validated_imd validate(postprocessed_img) forgery_detect(img)

```
{                                   a=dct_of_img()
b=lexicographically_sort_of_vectors(b)   //
Compares the size, colour of the image orderly
one by one.          c=correlation_of_vectors(c)
//Satisfaction relation between two images.
}
```

Fig 4.3: Steps of preprocessing

c) Feature Extraction :-

Feature Extraction comprises of extracting the essential features from the image, It effectively capturing the block size, length, color, height, width, threshold number of the image using Copy-Move Forgery (CMF).

Steps involved in CMF :-

a. Preprocessing :-The process analyze the image.

Preprocessed_img = prepro- cessing(img)

b. Block division :- divide the image into several blocks.

Blocks = di- vide_into_blocks(preprocessed_img

c. Feature extraction :- The specific features of image are extracted like size, color etc.

Features = extract_features(blocks)

d. Block matching :-This process match the particular block with the image. Matched_blocks = match_blocks(features)

e. Detection of forged regions :- Detects the tampered or altered part of image. Forged_regions = detect_forged_regions(matched_blocks)

f. Post-preprocessing :- This process analyze image after all steps are executed. Postprocessed_img = postprocess(forged_regions)

g. Validation :- Validate the image.

h. Fig 4.4: Pseudocode of CMF

d) CNN Model :-

CNN is a deep learning algorithm, specially designed for working with images. Algorithm is mainly used for classification and detection.

1. Start
2. Import the required libraries like Tensorflow and Keras.
3. Define the 'create_model' function, The function takes 2-parameters as 'input_shape' and 'num_classes'.
4. Initialize the sequential model. Create an instance of 'keras.models.sequential'.
5. Add all the CNN layers
   a. Convolution layer
   b. Max-pooling layer
   c. Fully connected layer
6. Add the output dense layer and return the model. 7. End

Fig 4.5: Algorithm for CNN model

The above figure 4.5 explain the brief steps in CNN algorithm, which start with importing the required libraries than create the model function using 2-parameters such as input shape and number classes, then initialize the sequential model and add all the CNN layers and dense layer which gives the output model.

e) Classification :-

Classification is the last step, proposed method will extract features from the image and mapping them with a corresponding output, gives output as forged and non-forged image**.**

Fig4.6: Original Image

In above figure 4.6 classifies the original image, which have not been forged or altered.

Fig4.7: Forged Image

The above figure 4.7 classifies the output of forged or manipulated image, image is tampered by using several tools like pixel, snapshot etc.

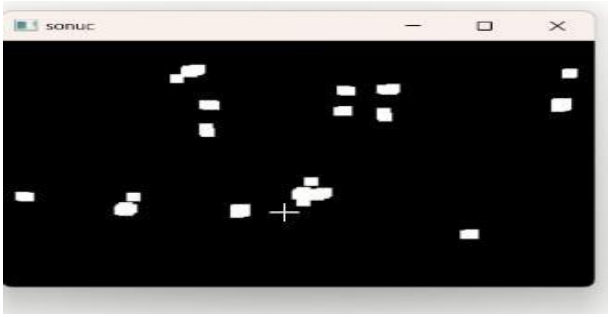

Fig4.8: The Forged Places

The above figure 4.8 shows the forged image spaces, means where the particular image is forged using several tools and techniques.

5. RESULTS

The outcomes of proposed methodgiveaccuracy and loss of every image.

Accuracy:- Classifies how the images are distinguish between forged and not forged and gives accurate results.

$$\text{Accuracy} = \frac{\text{Number of classified images}}{\text{Total no.of images}} \times 100\%$$

Loss:- Identifies how much particular image is wrong.

Loss = (y*log(p)+(1-y)*log(1-p) Where, p is model' s prediction andY is true label.

Methods	Accuracy	Precision	Recall
CMF	0.8564	0.428	0.205
ELA	0.6743	0.757	0.283
TL	0.7560	0.526	0.662
CNN	0.7580	0.589	0.562
Proposed	0.9800	0.980	0.872

Fig 5.1: Epoch values

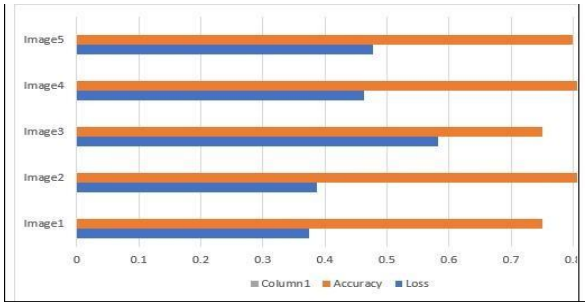

Fig 5.2: Accuracy and Loss Graph

The above graph shows the accuracy and loss graph of images. Where x-axis is the values and y-axis are images.

6. CONCLUSION

The best method for preventing different public difficulties is the deep learning assessment of picture falsification detection. As we covered in this study, the CNN model and CMF technique will be used in deep learning-based image forgery identification. This is a method that iscurrently in use and shows promise for a number of real-world uses. The method of gathering data may get harder as technology advances. We can easily detect image forgeries by using the CNN model, which gives us control over the power of forgery tools. This research will produce accurate results about 98% of the time, which is more sustainable for people as a whole.

7. FUTURE ENHANCEMENT

The image forgery detection using deep learning approach is robust and transparent, making it as valuable tool to avoid the misleading information on social media, this work can be improved in future as real time detection using AI tools and techniques.

REFERENCES

1 Dr.K.Prasanthi **"**Image Forgery Detection", IJCRT, Vol. 11, pp. f450-f453, Mar. 2023.

2 Dubey Krishna, "Image Forgery Detection Website", International publication of Research Publication and Reviews, Vol. 4, pp. 2146-2150, Oct. 2023.

3 Natarajan, P. BusterNet, "Image Copy-Move Forgery Detection with Source/Target Localization," Euroconference on Application of Computer Vision, pp. 2328, Aug. 2020.

4 P. He, H. Li, "Detection of fake Images", International Conference on Emerging Trends IEEE, pp. 22992303, 2019.

5 Amit Doegar. , "Image Forgery Detection leveraging Google Net and Random Forest algorithm", Journal of University of Shanghai, Vol. 22, pp. 1271- 1278, Dec. 2020.

6 Amit Doegar , "Image Forgery Detection derived from fusion of lightweight deep learning models"**,** Turkish Journal of EECS, Vol. 29, pp. 1978-1993, Mar 2021.

7 Ashgan H. Khalil, "Enhancing Digital Image Tampered Detection Using Transferearning**",** IEEE, 2023. Pune, pp. 78-84

8 Sankalp Patekar , "Image Forgery Detection**",**
Journal for Basic Sciences, Vol. 23, pp. 114-121, 2023.

9 Preethi Sharma, et al, "Comprehensive assessment of Image Forgery Detection", Vol. 82, pp. 18117-18150, Oct. 2022.Emad UI Haq Qazi ,

10 "Deep Learning based Image Forgery Detection**",** IASC, Vol. 38, pp. 225-240, Feb.2024.