Int. Jrl. of **Computational Learning & Intelligence**
Vol. 02, Issue 03 (July), 2023

RESEARCH ARTICLE

Image Forgery Detection Using Ensemble of VGG-16 and CNN Architecture

Smitha B N . G T Mohan Kumar . Manjushree H C . Abhishek M . Nallabothula Sneha

Department of Computer Science and Engineering,
Sai Vidya Institute of Technology, Yelahanka, Bengaluru, India.
DOI: 10.5281/zenodo.8210388

Received: 28 June 2023 / Revised: 06 July 2023 / Accepted: 27 July 2023

Abstract – Digital image modification or image forgery is easy to do today. The authenticity verification of an image becomes important to protect the image integrity so that the image is not being misused. Error Level Analysis (ELA) can be used to detect the modification in image by lowering the quality of image and comparing the error level. The use of deep learning approach is a state-of-the-art in solving cases of image data classification. This study wants to know the effect of adding ELA extraction process in the image forgery detection using deep learning approach. The Convolutional Neural Network (CNN), which is a deep learning method, is used as a method to do the image forgery detection.

Index Terms – Deep Learning, Convolutional Neural Networks, Error Level Analysis, Image Processing, Image Forgery.

I. INRODUCTION

Image data is extremely prone to manipulation in today's digital environment. Image editing software is widely available today, and it may be used not only on desktop computers and laptops, but also on handheld mobile devices. A deep generative model is commonly used to create hyper-realistic face-swapping images and videos in some applications. People commonly exploit the outcomes of this image manipulation on social media, in the commercial world, and even for criminal purposes. The use of image manipulation for illegal purposes should be a major source of concern, since it can pose a serious threat to society, government, and industry. As a result, the validity of the images in the internet must be confirmed. So that, maintaining the integrity of digital photographs is crucial. In this situation, an image forgery detection method can be used to verify the validity of digital images. The Digital Image Forensics (DIF) is a field to detect the authenticity of digital images, both in terms of the image content's integrity and the source. Active and passive

modification detection techniques are two types of algorithms for detecting picture forgery in DIF. The method of passive forgery detection does not need any prior knowledge of the image's content. The active technique, on the other hand, requires extracting watermarks and digital signatures embedded in images and then verifying them. As a result, any modification to the image can disrupt the embedded watermark and digital signature, assisting in the detection of the image's validity. The copy-move (cloning) modification method is the passive image forgery that has the largest impact on the original image.

II. RELATED WORK

Image Forgery is not a modern concept as it comes along with the invention of photography. But it comes in the limelight nowadays, with the invent of easily accessible digital cameras supported with image editing software tools. Image Forgery begins with the first known fake image that was of Hippolyta Bayard, who released a fake picture of him committing suicide as an act of annoyance for the sake of losing the tag of inventor of photography to Louis Daguerre in 1840 [1]. Digital visual media, nowadays, represent one of the prominent technique of exchanging information, because of increase in easy to use and inexpensive devices. Moreover, visual media has greater expressive potential than any of the existing media. It describes convoluted scenes in an uncomplicated manner, whichever in a different way can be quite tough to transcribe. Malicious modification of digital images with intent to deceive for the sake of altering the public perception is termed as Digital Image Forgery.

The modification is done in such a way that it hardly leaves any visually detectable traces. Manipulation of Digital images is not any longer defined to experts with all the arrival and dispersal of handy image editing tools and softwares. Some of the well-known images editing tools available online are Sumopaint, Paintshop Pro, Photoshop CC, HitFilm Express. Manipulation of visual media with such easily available tools is no longer a herculean task. It is not concerned whether an image is fake or not, until or unless it causes some harm. These images are accepted as certification of truthfulness almost by everyone and everywhere. So, confirmation of an images authenticity is needed. Such confirmation is done with the help of image forgery detection techniques. These methods aim at validating the authenticity of images. There are several types of image forgery exposed to date and correspondingly the forgery detection techniques. This paper aims to review the existing types of forgeries and their detection techniques.

Need of Digital Image Forgery Detection

In today s world, it has become so easy to access, process, store and share the information with the availability of handy devices by everyone. Image editing software tools are increasing day by day, leading to the forgery of digital images. The rapid increase in forged images leads to decrease of trust in visual media. Easiness in simulating origin and content of digital visual information, the trustworthiness has always been questioned. It raised the need for forgery detection

techniques due to the significant impact of image manipulation on medicine, justice, news reporting and accounting professions. Forgery detection techniques aim to identify inconsistent patterns which are supposed to be present in the image because of manipulation is done in order to forge the image. Active and passive are the two approaches used for detecting forgery in images. The active approach requires prior information about the image to be embedded into the image itself by using Digital Signature or Digital Watermark in order to detect any manipulation. The passive approach requires no such information about the image to authenticate it. It assumes the fact that although tampering won't leave any visual trace, but they are more likely to modify the image statistics, and these underlying inconsistencies play key role in detection of tampering.

An example of digital image forgery is shown in Figure 1. In this image Malaysian politician Jeffrey Wong Su En was seen being knighted by the Queen of England in July 2010. In Figure 1b the original image was, later on, found out to be of Ross Brown, Formula One Managing Director of Motorsports, accepting the Order of the British Empire from the Queen. Figure 1a later on, found out to be spliced, of Mr.Wongs face and an original ceremony photo, to expand Mr. Wongs fame. Another example of digital image forgery is shown in Figure 2. A leading national party spokesperson shared an image on an Indian news channel which later on found out to be forged as shown in Figure 2a.

The original image was an iconic image taken by photojournalist Joe Rosenthal in 1945 titled Raising the flag at Iwo Jima taken during World War II as shown in Figure 2b. Digital Image Forgery tends to alter the public perception by representing such things which do not even exist. Forgery Detection Techniques aim to verify the authentication of all such information so that it does not mislead the public. Nowadays, every country is adopting the paperless workplaces which lead to storage of data virtually or in digital format, which makes it more vulnerable to get manipulated. It raises the concern of data security. So, researchers took a keen interest in securing.

(a) Forged Image (b) Original Image

Figure1

(a) Forged Image (b) Original Image

Figure 2

III. SYSTEM ARCHITECTURE

Image forgery is caused by different forgery techniques like image splicing, copy-move etc.... To detect this forgery firstly dataset of different images is collected and processed and

trained. When the input images are given it is trained and the algorithm is applied to get the output.

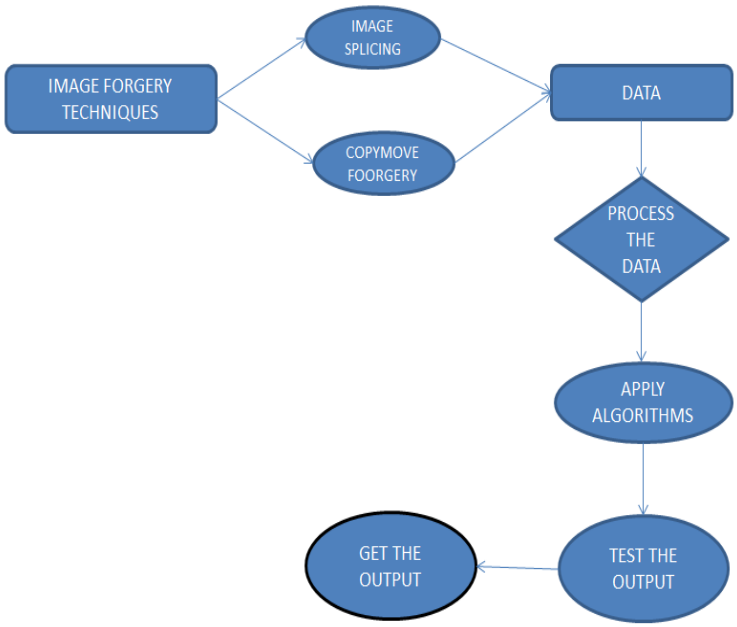

Figure.3: System Architecture

IV. METHODOLOGY

The dataset we get is through kaggle website. Inside there are 2337 images belonging to two classes. The size of the dataset is changed to 224x224 pixels. In this experiment, we divide the dataset into two namely training set and test set. In the range 80-20% for the training set and the rest is used for test data. In compiling the dataset, we divide the data train and test data each of which there are 2 categories, namely the category of fake images and the original image. The first step we took was to divide the dataset from into 2 categories: Original and fake images. We normalize the image by processing the image to a size of 224x224 pixels. Then our next step is to perform analysis on the level of compression error image, from the compression result then we use the VGG 16 architecture for CNN in recognizing the original image and forgery images according to the ELA. Our next step is to summarize the results of the training. Our proposed method described on flowchart.

CNN

Convolutional Neural Networks have a different architecture than regular Neural Networks. Regular Neural Networks transform an input by putting it through a series of hidden layers. Every layer is made up of a set of neurons, where each layer is fully connected to all neurons in the layer before. Finally, there is a last fully-connected layer — the output layer — that represent the predictions. Convolutional Neural Networks are a bit different. First of all, the layers are organised in

3 dimensions: width, height and depth. Further, the neurons in one layer do not connect to all the neurons in the next layer but only to a small region of it. Lastly, the final output will be reduced to a single vector of probability scores, organized along the depth dimension.

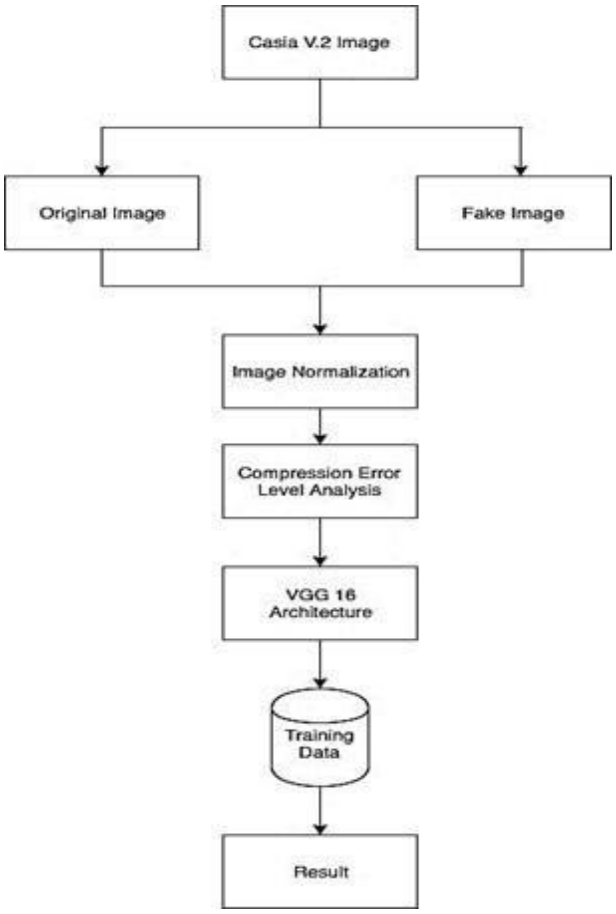

Figure. 4: Methodology cum Flow Chart

- **Module 1: Region Proposal**. Generate and extract category independent region proposals, e.g. candidate bounding boxes.
- **Module 2: Feature Extractor**. Extract feature from each candidate region, e.g. using a deep convolutional neural network.
- **Module 3: Classifier**. Classify features as one of the known class, e.g. CNN classifier model.

Collection datasets

- We are going to collect datasets for the prediction from the kaggle.com
- The data sets consists of Image Forgery detection Classes

Data Pre Processing

- In data pre-processing we are going to perform some image pre-processing techniques on the selected data
- Image Resize
- And Splitting data into train and test

Data Modelling

- The split train data are passed as input to the CNN algorithm, which helps in training.
- The trained skin image data evaluated by passing test data to the algorithm
- Accuracy is calculated

Build Model

- Once the data is trained and if it showing the accuracy rate as high, then we need to build model file

CNN

A convolutional neural network is a feed-forward neural network that is generally used to analyze visual images by processing data with grid-like topology. It's also known as a ConvNet. A convolutional neural network is used to detect and classify objects in an image.

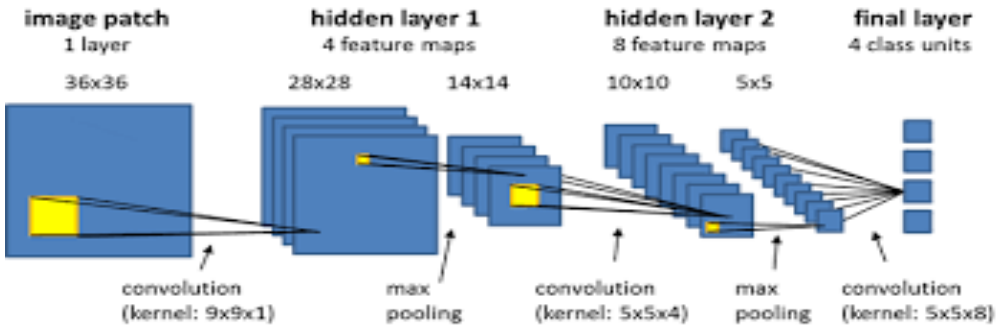

Figure. 5: Layers of CNN

Convolutional Neural Networks have the following layers:

- Convolutional
- ReLU Layer
- Pooling
- Fully Connected Layer

Step1: Convolution Layer:

Convolutional neural networks apply a filter to an input to create a feature map that summarizes the presence of detected features in the input.

Step2: ReLU Layer

In this layer, we remove every negative value from the filtered images and replaces them with zeros. It is happening to avoid the values from adding up to zero. **Rectified Linear unit (ReLU)** transform functions only activates a node if the input is above a certain quantity. While the data is below zero, the output is zero, but when the information rises above a threshold. It has a linear relationship with the dependent variable.

Step3: Pooling Layer

In the layer, we shrink the image stack into a smaller size. Pooling is done after passing by the activation layer. We do by implementing the following 4 steps:

- Pick a **window size** (often 2 or 3)
- Pick a **stride** (usually 2)
- **Walk** your Window **across** your **filtered** images
- From each **Window**, takethe **maximum** value

Step4: Fully Connected Layer

The last layer in the network is **fully connected**, meaning that neurons of preceding layers are connected to every neuron in subsequent layers. This **mimics high-level reasoning** where all possible pathways from the input to output are considered. Then, take the shrunk image and put into the single list, so we have got after passing through two layers of convolution ReLU and pooling and then converting it into a single file or a vector.

V. VALIDATION

Toward the consummation of the reconciliation testing, the product is totally amassed as bundle interfacing blunders have been revealed and adjusted and a last arrangement of programming tests starts in approval testing. Approval testing can be characterized from multiple points of view, however a straightforward definition is that the approval succeeds when the product work in a way that is normal by the client. After approval test has been directed as follows:

- The capacity or execution qualities adjust to detail and are acknowledged.
- A deviation from the particular is revealed and a lack list is made.

- Proposed framework viable has been tried by utilizing an approval test and discovered to be working acceptably.

VI. TEST REPORTS

The users test the developed system when changes are made according to the needs. The testing phase involves the testing of the developed system using various kinds of data. An elaborate testing of data is prepared and system is tested using the test data. Test cases are used to check for outputs with different set of inputs.

Test Cases :

Test Case	Test Purpose	Test condition	Expected outcome	Actual result	Pass or Fail
Load Images data	Upload Image Forgery images data	Check for Image Forgery data	Uploaded successfully	Image is loaded Successfully.	Pass
Pre -Processing	Apply methods like, noise removal, gray conversion	Pre-processing for image	Frames are converted successfully	As Expected.	Pass
Apply feature classification using cnn	Feature extraction is done for pre processed image	Check for feature extraction	Feature extraction data is complete	As Expected.	Pass
Detecting object using neural network	Train model	Check for model loss and accuracy	Model trained successfully	Model trained successfully	Pass
Image Forgery image as input	Detection the given object	Check for Image Forgery classification with accuracy	Predicted result	Result is shown.	Pass

VII. CONCLUSION

This paper solves the problem of distinguishing real images and forgery images using deep learning. We propose a new system from combination Error Level Analysis and Convolutional Neural Network in machine learning and computer vision to solve the problems above. First, we divide the dataset into tampered images and original images, then we determine the architecture that will be used to train the recognition. We chose to use CNN in this training because CNN is perfect

for training with minimal datasets. The result of our experiment is that we get the best accuracy of training 96.8% and 88.46% of validation.

REFERENCES

1. Kuznetsov, A. (2019, November). Digital image forgery detection using deep learning approach. In *Journal of Physics: Conference Series* (Vol. 1368, No. 3, p. 032028). IOP Publishing.
2. Doegar, A., Dutta, M., & Gaurav, K. (2019). Cnn based image forgery detection using pre-trained alexnet model. *International Journal of Computational Intelligence & IoT*, *2*(1).
3. Nagashree, N., Patil, P., Patil, S., & Kokatanur, M. (2021, June). Alpha beta pruned UNet-a modified unet framework to segment MRI brain image to analyse the effects of CNTNAP2 gene towards autism detection. In *2021 3rd International Conference on Computer Communication and the Internet (ICCCI)* (pp. 23-26). IEEE.
4. Diallo, B., Urruty, T., Bourdon, P., & Fernandez-Maloigne, C. (2020). Robust forgery detection for compressed images using CNN supervision. *Forensic Science International: Reports*, *2*, 100112.
5. Kumar, S. S., Ahmed, S. T., Xin, Q., Sandeep, S., Madheswaran, M., & Basha, S. M. (2022). Unstructured Oncological Image Cluster Identification Using Improved Unsupervised Clustering Techniques. *Computers, Materials & Continua*, *72*(1).
6. Mallick, D., Shaikh, M., Gulhane, A., & Maktum, T. (2022). Copy move and splicing image forgery detection using cnn. In *ITM Web of Conferences* (Vol. 44, p. 03052). EDP Sciences.
7. Syed Thouheed Ahmed, S., Sandhya, M., & Shankar, S. (2018, August). ICT's role in building and understanding indian telemedicine environment: A study. In *Information and Communication Technology for Competitive Strategies: Proceedings of Third International Conference on ICTCS 2017* (pp. 391-397). Singapore: Springer Singapore.
8. Varchagall, M., Nethravathi, N. P., Chandramma, R., Nagashree, N., & Athreya, S. M. (2023). Using Deep Learning Techniques to Evaluate Lung Cancer Using CT Images. *SN Computer Science*, *4*(2), 173.
9. Huang, N., He, J., & Zhu, N. (2018, August). A novel method for detecting image forgery based on convolutional neural network. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1702-1705). IEEE.
10. Al-Shammari, N. K., Syed, T. H., & Syed, M. B. (2021). An Edge–IoT framework and prototype based on blockchain for smart healthcare applications. *Engineering, Technology & Applied Science Research*, *11*(4), 7326-7331.
11. Nagashree, N., Patil, P., Patil, S., & Kokatanur, M. (2022). InvCos curvature patch image registration technique for accurate segmentation of autistic brain images. In *Soft Computing and Signal Processing: Proceedings of 3rd ICSCSP 2020, Volume 2* (pp. 659-666). Springer Singapore.
12. Qazi, E. U. H., Zia, T., & Almorjan, A. (2022). Deep learning-based digital image forgery detection system. *Applied Sciences*, *12*(6), 2851.

Appendix

Table A1:Literature Survey and Reviews

Title	Author	Objective	Methodology	Results	Advantage
Image forgery detection review	Hiba Benhamza Abdelhamid Djeffal Abbas Cheddad	In the proposed method this issue has been addressed without compromising the quality of the method. Discrete Cosine Transform (DCT) is used to represent the features of overlapping blocks.	After the tremendous development in communication technologies in last recent years, digital image forgery detection has become a centre of interest for many scientific researchers trying to secure many administrative and business activities. Indeed, scientific research is now aware of the proposition of several techniques for the detection of falsified documents, especially passive methods. Image forgery detection is concerned with detecting manipulated images or verifying their authenticity. It is divided into two main categories: Active and passive. A. Passive	We studied that, due to the advancement in the digital software's manipulation of digital images has become easy. As powerful computers, advanced photo-editing software packages and high resolution capturing devices are invented	The proposed method has addressed the issue successfully and is considerably faster than the existing method. It has detected forgery with good success rate in the image dataset. Also, it has shown robustness against Added Gaussian noise, JPEG compression and small amount of scaling and rotation

Appendix

			methods Passive forgery detection techniques do not need any signature or watermark to detect forgery but rather by analysing the statistical distortion they leave behind after forgery although the detection of digital image falsification in this case is considered more difficult. This technique has become widely used because it does not need prior information about the image. It depends on the hypothesis that any modification in the image may change its consistency or statistics property		
Image forgery detection: a survey of recent deep-learning approaches	Marcello Zanardelli Fabrizio Guerrini Riccardo Leonardi	The classification is based on documents type, forgery type, detection method, validation dataset, evaluation metrics and obtained results. Most of existing forgery detection works are dealing with images and few of them analyze administrative documents and go deeper to analyze their contents.	Deep Fake methods We now present a few of the most recent DeepFake-specific detection methods, that achieved the best results on the previously introduced datasets for DeepFakes detection evaluation (see Section 3.1). The selection has been made according to the criteria previously outlined, namely, suitability for the still images case.	This report presents main existent works related to image and document forgery detection and introduces their methods, results and discussion. The aim of this report is to point the main challenges of this research field and to compare the proposed methods and discuss their advantages and limits.	This paper is considered as a survey to start a work on detecting forgery in Arabic administrative documents by analysing them and preparing a training image dataset

Appendix

Image Forgery Detection Using Deep Learning by Recompressing Images	Syed Sadaf Ali Iyyakutti Iyappan Ganapathi Ngoc-Son Vu	The proposed model is lightweight, and its performance demonstrates that it is faster than state-of-the-art approaches. The experiment results are encouraging, with an overall validation accuracy of 92.23%.	we introduce a robust deep learning based system for identifying image forgeries in the context of double image compression. The difference between an image's original and recompressed versions is used to train our model.	The proposed model learns the existence of the forgery in an image through the numerous artifacts left behind during image forgery. The trained model can identify tampering with high accuracy	The proposed technique can efficiently detect image splicing and copy-move types of image forgeries. The experiments results are highly encouraging, and they show that the overall validation accuracy is 92.23%
Image Forgery Detection and Deep Learning Techniques: A Review	Ritu Agarwal Deepak Khudaniya Abhinav Gupta	The paper initially discusses various types of image forgery techniques and later on compares different approaches involving neural networks to identify forged images.	This has led researchers to work on various techniques for the detection of manipulated images with improved accuracy. Traditional works on image forgery detection are mostly based on extracting simple features that are specific for detecting some	1. Deep Learning methods performfar better than traditional methods as they can extract hidden features, thus they give higher levels of accuracy. 2.These methods are flexible and can be modified a little to	The paper discusses basic CNN architecture which is used by most deep learning approaches. Further, a comparative analysis of various deep learning methods, their effectiveness,

Appendix

			particular type of forgery. Recently, works on forgery detection based on neural networks have proved to be very efficient in detecting image forgery. Neural networks are capable of extracting complex hidden features of an image, thus giving better accuracy	be used for different types of forgery detection.	and their limitations are discussed.
Image Forgery Detection by using Machine Learning	J.Malathi, B.Narasimha Swamy, Ramgopal Musunuri	In this paper, we propose a two phase imperative altering way to deal with oversee direct learn featuresin referencing to see changed pictures in various pictureformats	This proposes the structure does notwork always transversely over different evolving frameworks. Mix of no under two pictures to make a completely phony picture is known as Image structure. It winds up being difficult to disengage between certified picture and phony picture in light of the closeness of different astounding changing programming endeavors	This work is basically fit for seeing joined pictures. As future work, we will join other picture changes, for instance, DCT as the base intertwine information	This will draw in the essential understudy to modify more qualities of changed zones and ensurebetter exactness for balanced region control transversely over different image file formats.
Digital image forgery detection using deep learning approach	A Kuznetsov	The proposed network architecture takes image patches as input and obtains classification results for a patch: original or forgery. On the training stage we select patches from original image	The proposed network was trained for 300 epochs (Figure 2 shows the training process). At the testing stage, patches were extracted using the same methodology used for training, while the final decision on image classification is made by	The obtained results demonstrate high classification accuracy (97.8% accuracy for fine-tuned model and 96.4% accuracy for the zero-stage trained) for a set of images containing artificial distortions in comparison	The results obtained showed a high quality of image classification (97.8% accuracy for finetuned model and 96.4% accuracy for the zero-stage trained) and the possibility of applying the method under conditions of repeated compression of

Appendix

		regions and on the borders of embedded splicing	voting on the majority of patches of the first or second class.	with existing solutions. Experimental research was conducted using CASIA datase	distorted images by the JPEG algorithm
Image Forgery and it's Detection Technique: A Review	Varsha Sharma, Swati Jha , Dr. Rajendra Kumar Bharti	Block matching algorithm or block tiling algorithm is the most commonly used method to detect the duplication in the image. One of the major challenges is the time complexity of such algorithms.	In the proposed method this issue has been addressed without compromising the quality of the method. Discrete Cosine Transform (DCT) is used to represent the features of overlapping blocks	The proposed method has addressed the issue successfully and is considerably faster than the existing method. It has detected forgery with good success rate in the image dataset	The proposed method uses the DCT coefficients to represent the overlapping block. The DCT coefficients are ordered in zigzag manner to keep the low frequency coefficients together and before the high frequency coefficients in the row vector.
Image copy-move forgery detection and localization based on super-BPD segmentation and DCNN	Qianwen Li, Chengyou Wang, Xiao Zhou & Zhiliang Qin	an image copymove forgery detection and localization based on super boundary-to-pixel direction (super-BPD) segmentation and deep CNN (DCNN) is proposed: SD-Net. Firstly, the segmentation technology is used to enhance the connection between the same or similar image blocks, improving the detection accuracy	this paper proposes an image CMFD based on super boundary-to-pixel direction (super-BPD) segmentation and deep CNN (DCNN): SD-Net. To obtain suitable and global CMFD features, DCNN is used to extract image features, replacing conventional hand-crafed features with automatic learning.	The super-BPD segmentation technology is used to improve edge detection accuracy. Te DCNN is used to improve method robustness	The method that reduce complexity while ensuring accuracy is need be investigated in the future. Moreover, detecting forgery with similar but real regions also requires deep exploration.