JCST Journal of Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777787

OVERVIEW OF IMPROVED COPY-MOVE FORGERY DETECTION TECHNIQUES BASED ON DEEP LEARNING

K. Anusha[1]V. Kamakshi Prasad[2]
[1] Research Scholar, JNTU, Hyderabad,anusha.jntuh@gmail.com
[2] Professor of CSE, JNTU, Hyderabad, kamakshiprasad@jntuh.ac.in

Abstract. In recent years, the development of fake or forged digital images is common by applying different popular image editing tools such as adobe photoshop, affinity photoshop, CyberLink photo director 365, and by using high-resolution capturing devices. It is difficult to differentiate between the original and tampered or fake images. Copying and relocating one or more sections of an image within the same image is referred to as copy-move forgery, which has become a prevalent form of forgery in contemporary times. Conventional techniques for detecting copy-move forgery (CMFD) can be broadly classified into two categories. One is using block-based methods and the other is key point-based methods. These methods have their limitations such as the computational cost being high because of the large amounts of data, and the high error rate in smooth areas of the image. Further these are less robust against pre-processing or post-processing operations and scaling attacks. A lot of research has been done and many techniques exist to localize the forged image and to detect the forged region of images. In this paper, the survey is made on the recent developments in copy move forgery detection techniques using deep learning. Additionally, we explore different benchmark datasets that have been employed by various techniques for the detection of copy-move forgery. We also discuss key aspects and comparison of various deep-learning techniques which are used to detect copy-move image forgery.

Keywords: Convolutional Neural Networks, Image forgery, Copy move forgery, Deep learning

Introduction

Images and videos are basic sources of information and they are important in today's world. Because of global internet usage, there is an increase in the emergence of using social media. Image documents have a significant role in diverse fields such as newspapers, criminology research, medical imaging, court evidence, press photography, military operations, intelligence, and in different other applications. Thus, the legitimacy of an image has an important role as they are eminently used as shreds of evidence in a wide range of applications.

Expansion and quick development of many image editing software tools like Adobe Photoshop, GIMP, PIXLR made the process easy to spread false information by forging or manipulating images [1]. Digital images are not acceptable as proof of evidence in courts without proper forensic analysis. Consequently, the legitimacy of a digital image is an active research area in multimedia security. Digital image authentication techniques are classified into two types: i) Active authentication, and ii) Passive authentication. Active authentication methods require additional information to be added using either a digital signature or a watermark to the original images by an authorized person. The embedded information acts as metadata and the same is used for manipulation detection in the images. Metadata could be altered or substituted by the malicious user which is a serious drawback of active authentication. Though robust methods like fragile watermarking [2] and robust signatures [3] detect the manipulation in the images and still faces some problems associated with metadata.

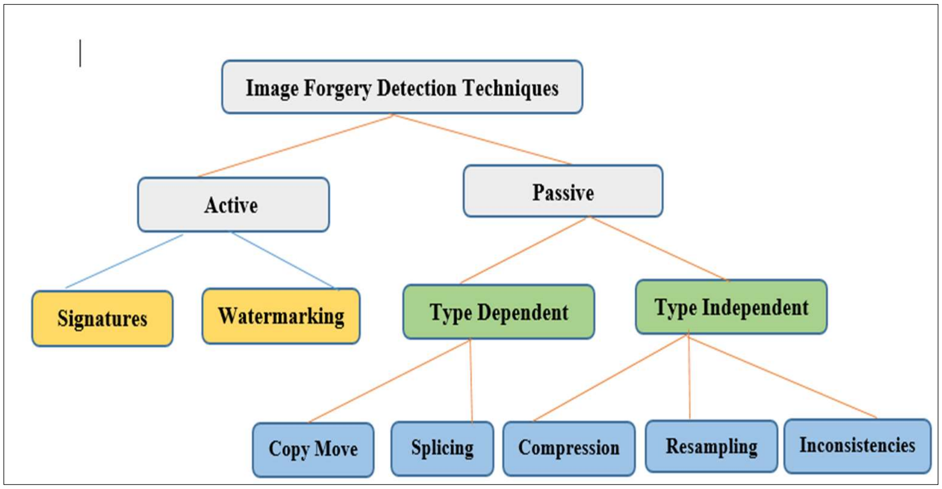


Fig. 1. Classification of image forgery detection methods

A passive authentication technique doesn't require any additional metadata to determine the forgery in images. Passive techniques are referred to as forensics [4] and are also called blind approaches. They aim to examine the images themselves and identify the traces of tampered image. Classification of image forgery detection methods has been illustrated in Fig. 1.

2. Image Forgery Types

There are many ways to tamper the digital images by adding unusual patterns, modifying image features, and removing objects from the images.

Copy-move Forgery: The process of duplicating a particular scene within an image by copying and pasting one or more sections (regardless of their size) to a different region of the same image is known as copy-pasting forgery. As illustrated in Figure 2a, an additional ladybug has been inserted as a duplicate of the one in the left image.

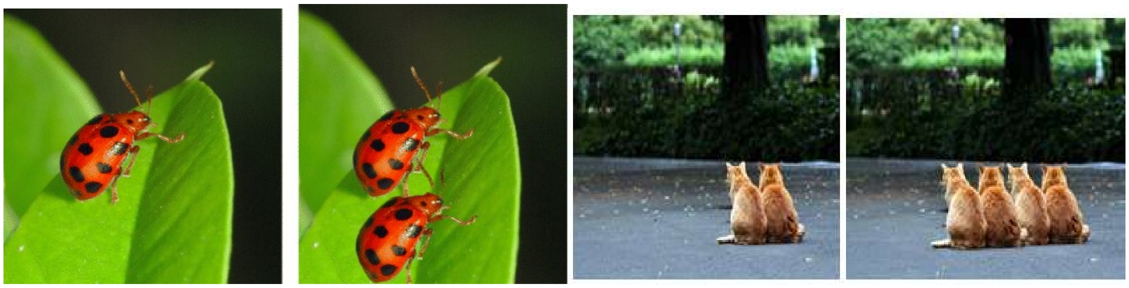
Image Splicing: It is same as copy-move forgery, with a notable difference that merging or adding different parts of the images into one image to make a fake situation. An example of image splicing attack on images is shown in Fig. 2. Two different images are composed and created a new image.

DeepFakes: This is a kind of altering, creating convincing images or creating fake content in videos or images using artificial intelligence called deep learning. Before deep learning, this task was done by expert professionals using various editing tools, now it is automated by deep learning models, using autoencoders, and GANs [5].

CGI- generated images/videos: Computer Generated Imagery is a form of creating 3D realistic photos as the rendering output which is undistinguishable from original photos. In recent years, CGI is useful in various fields like real estate, movies, advertising, crowdfunding, etc., consequently, millions of images or videos getting produced every day.

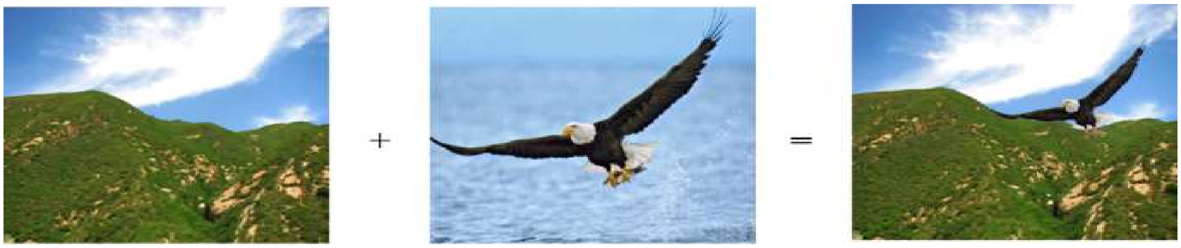
Consequently, these images are indistinguishable from real images taken with high-end resolution devices, the example for this type of images are shown in Fig. 5, and these images can be used for malicious activities.

Retouched forgery: Some features of the images are enhanced by changing the brightness, color, and contrast of the image.



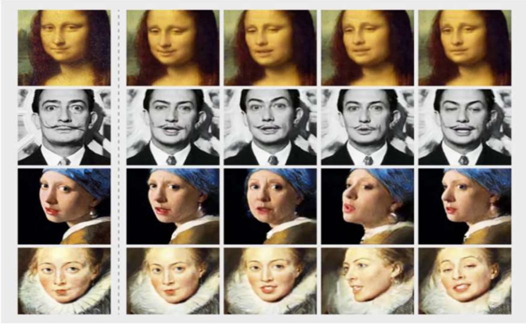
i) ii) iii) iv)

Fig. 2. Copy-move forgery: i& iii are original images ii) & iv) are tampered images



i) ii) iii)

Fig. 3. Image splicing forgery: i) & ii) are original images and iii) tampered image



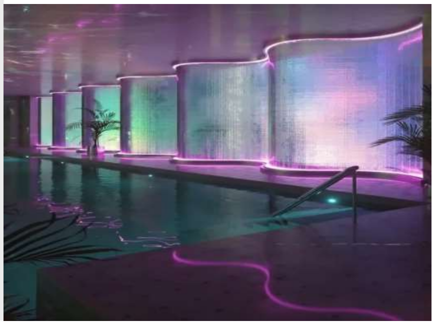


Fig. 4. Deepfakes: The first column shows the original image and the remaining four are DeepFakes obtained.

Fig. 5. CGI-rendered (Photo from Reddit)

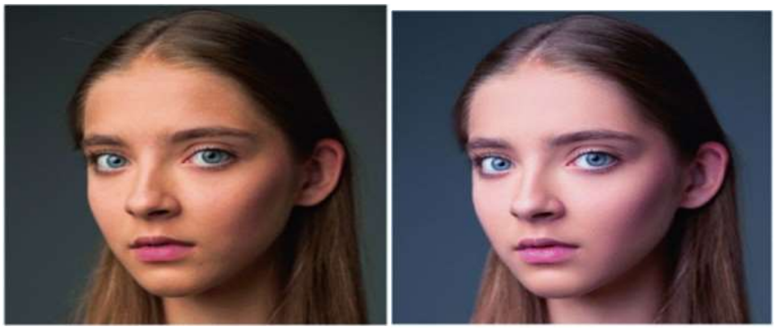


Fig. 6. Original image Retouched image

3. Datasets Description

In their study to address important benchmarking databases which are popular and commonly used in copy-move forgery and image-splicing attacks.

CMFD [6] dataset composed of forty-eight original images of size (2300 x 3000) in JPEG and PNG formats and with different content.

CoMoFoD [7] dataset contains 260 image sets, among them, 200 images are in the small image category which is in size (512x512), and 60 images in the large image category (3000 x 2000). Various transformations such as rotation, scaling, distortion, combination, translation, and post-processing operations like brightness change, contrast adjustments, JPEG compression, etc. are applied to both original and tampered images.

CASIA V1.0 [8] benchmarking dataset contains images of size 384 x 256 in JPEG format. It contains 1721 images, of these 800 are original images and 921 are tampered images.

CASIA V2.0 [8] dataset contains 7,492 original images, and 5,123 tampered images of different sizes. The sizes vary from 240 x 160 to 900 x 600. This dataset deals with different formats such as JPEG, TIF, and BMP. It deals with both splicing and copy-move forgery attacks.

MICC-F2000 [9] dataset consists of a total of 2,000 images, with 1,300 being original images and 700 being forged images. All the images are in JPEG format and have a resolution of 2048 × 1536 pixels.

MICC-F600 [9] It consists of 160 tampered images and 440 original images with sizes varying from 722 x 480 pixels to 800 x 600 pixels and supports JPEG and PNG format.

SATs-130 [10] It comprises 96 images, 48 tampered and 48 original images of size between 1,024 x 683 and 3,264 x 2,448 pixels with JPEG format.

Korus [11, 12] It consists of images of size 1,920 x 1,080 in TIFF format. It contains 220 tampered images and 220 authorized images.

IMD [13] dataset consists of 48 authorized and 48 tampered images. The resolution of images is 3000 x 2300 in JPEG format.

All these datasets are summarized and shown in Table 1.

Table 1 Overview of datasets for copy-move forgery

Dataset	Manipulations	Size	No. of Original/ Forged images	Format
CMFD	Copy-move	various	0/48	JPEG, PNG
CoMoFoD	Copy-move	various	4800/4800	JPEG, PNG
CASIA V1.0	splicing, copy-move	384 x 256	800/921	JPEG
CASIA V2.	splicing, copy-move	240 x 160- 900 x 600	7492/5123	JPEG, TIFF
MICC-F2000	splicing, copy-move	2048 x 1536	1300/700	JPEG
MICC-F600	Copy-move	722 x 480- 800 x 600	440/160	JPEG, PNG
SATs-130	Copy-move	1024 x 683	48/48	JPEG
Korus	splicing, copy-move	1920 x 1080	220/220	TIFF
IMD	Copy-move	3000 x 2300	48/48	JPEG

4. Copy-move forgery detection techniques

Copying a single part or multiple parts of an image and pasting them in the same image at different parts of the image is known as a copy-move forgery. It is the most common type of forgery and is difficult to identify by human eyes as they copy a part from the same image, and because of its easy implementation. This approach duplicates the image with different features such as noise, rotation, and scaling, it is more problematic than retouching and splicing forgery attacks.

In general, there are two approaches to deal with copy-move forgery detection. One is based on conventional approaches like block-based techniques and key-point techniques and the other one is using deep learning approaches. Most conventional approaches rely on geometric or physical properties and image consistency to detect copy-move forgery whereas deep learning approaches rely on the creation of neural networks.

Both block-based and key-point based techniques in the conventional approaches followed a similar overall framework, depicted in Figure 7. The general framework comprised the following steps:

1. Perform pre-processing operations to enhance the structural changes on images.
2. Split or divide the image into circular or rectangular overlapping blocks.
3. Apply the feature extraction procedures on images and store them in feature vectors
4. Perform the localization of forged regions of an image to find the duplicates of the feature vectors.
5. Detect the forgery on images.

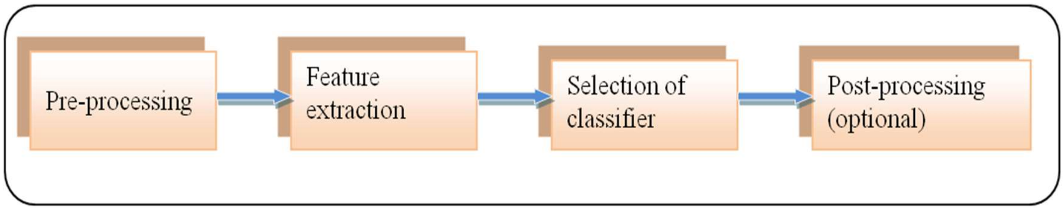


Fig. 7. General framework for copy-move forgery

4.1 Block-based Methods:

Based on various features, block-based methods are classified into four categories [13]. They are 1. Texture -based methods, 2. Moment invariant-based methods, 3. Dimension reduction-based methods, 4. Frequency transformation-based methods. Once the image is divided into circular, rectangular, or overlapped blocks various techniques are used on each block to extract features. Apply different feature extraction techniques such as Discrete Wavelet Transform (DWT), Dyadic Wavelet Transform (DyDWT), Fourier Transform (FT), and Discrete Cosine Transform (DCT) based on frequency transformations. Apart from the above techniques, moment invariant and texture invariant-based methods are also used to extract features from the images and to reduce the dimensionality of larger datasets, Principle Component Analysis (PCA) is used. B. Mahdian et. al [14] used hazy-shaped images to extract various changeless characteristics from image blocks. The block-based methods have several limitations. These methods are less robust to scaling attacks, have a high error rate for different images, and computational cost is high due to large amounts of data.

4.2 Key-point-based methods:

Key-point based methods depend on key-point descriptors to avoid image blocking. In these methods, the local characteristics identified from key points (near corners, edges, and spots) are used to analyze the image. Local features are extracted in the area near or surrounding a particular place. A comparison is made between the descriptors to detect the forged areas. D.G. Lowe et al. [15] used an algorithm based on Scale Invariant Feature Transform (SIFT) to extract constant features from the image. These features are invariant against geometrical attacks and post-processing attacks like JPEG compression, noise, and scaling. S. Prasad et al. [16] used the combination of SIFT, Speed Up Robust Feature (SURF), and Histogram Oriented Features (HOG) which are resulting in better accuracy compared to the individual performance of these features to detect the copy-move forgery.

In comparison, the computational complexity of feature mapping is relatively high when SIFT descriptors are used. Though SIFT descriptors reliably localize forged regions of an image, SURF [17] feature descriptors outperform SIFT descriptors because of their lower dimensions. On the other hand, keypoint-based approaches have a few limitations like natural duplicate objects are detected as fake duplicate objects. Both the approaches such as SIFT and SURF cannot detect small forged regions [18].

5. Deep-learning approaches for Copy-move forgery detection

In recent years, machine learning and deep-learning mechanisms gained huge popularity because of the advancement of algorithms to deal with scientific problems. Especially Convolutional Neural Networks (CNNs) outperform in the extraction of descriptive features automatically from the given input data. Deep learning mechanisms find application in various domains, including but not limited to object detection, image classification, image segmentation, medical imaging, face detection, and person re-identification. [19-20].

Compared to conventional approaches like block-based and key-point based methods, deep learning mechanisms perform better to identify copy-move forgery detection. In the following section, we present a detailed explanation of deep-learning architectures like segmentation and feature extraction, Contrast limited Adaptive Histogram Equalization (CLAHE) and CNN, Generative Adversarial Network (GAN) and CNN, Convolutional LSTM, and Quality Independent Deep Learning (QDL) to deal with copy-move forgery detection.

5.1 Segmentation and feature extraction using deep learning

The authors of [21] presented an algorithm specifically for copy-move forgery detection which uses deep learning to perform the segmentation and feature extraction from the images. A forged image is given as input to the system, and Simple Linear Iterative Clustering (SLIC) [22] is used to segment the input image as a pre-processing step, then performed the multi-scale feature extraction from segmented patches using one of the popular deep learning architectures for image processing called VGGNet (Visual Geometry Group-Net). After the feature extraction, Adaptive Patch Matching (ADM) is applied to blocks and the depth of each pixel is reconstructed to make the comparison between the blocks. After that skeptical forged regions are identified, and segmented patches of original images are merged. Finally forged region will be displayed as output.

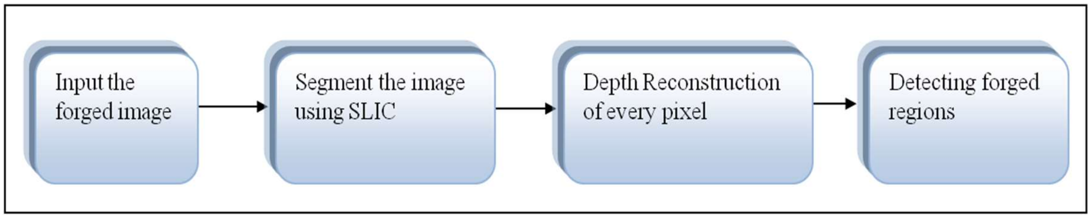

Input the forged image
Segment the image using SLIC
Depth Reconstruction of every pixel
Detecting forged regions

Fig. 8. The process flow of segmentation and feature extraction

The entire process shown in Fig. 8, is carried out in the following steps:

a. The color values of pixels and position of pixels in SLIC are built as the 5-D feature vector.
b. K-means clustering technique is used to estimate the similarity of these features, and to segment the superpixels.

c. The input image of size 224 x 224 is initialized to architecture like VGGNet where the feature extraction is performed by using the combination of the Convolution layer and Max-pooling layer.
d. A binary masking is applied on segmented superpixels for the given input image. Superpixel features are obtained by multiplying the binary mask with every channel. This process is repeated for each convolutional layer of VGGNet.
e. Single-scale features don't perform well as they could not obtain more information. Instead, multi-scale features are extracted using VGGNet, even if there exists a small variation between the original and tampered images.
f. Finally, Adaptive Patch Matching is used for comparing the associated features with copy-moved features by the superpixels to which the key point belongs.

This model trained the VGGNet and experiments were carried out on a MICC-F220 dataset which contains 220 images with 110 tampered and 110 original images. This model performance is subjected to only one dataset which consists of only a limited number of images. Copy move forgery hides certain image features by adding noise, coloring, and with other characteristics. To deal with hidden image features, a new deep learning architecture Contrast Limited Adaptive Histogram Equalization (CLAHE) is discussed in section 5.2.

5.2 Contrast-Limited Adaptive Histogram Equalization (CLAHE) and Convolutional Neural Network (CNN)

The authors of [13] presented a deep learning methodology designed for the purpose of classifying images as either original or forged in copy move forgery detection. To make the hidden features visible, contrast limited adaptive histogram equalization (CLAHE) was used with the combination of CNN.

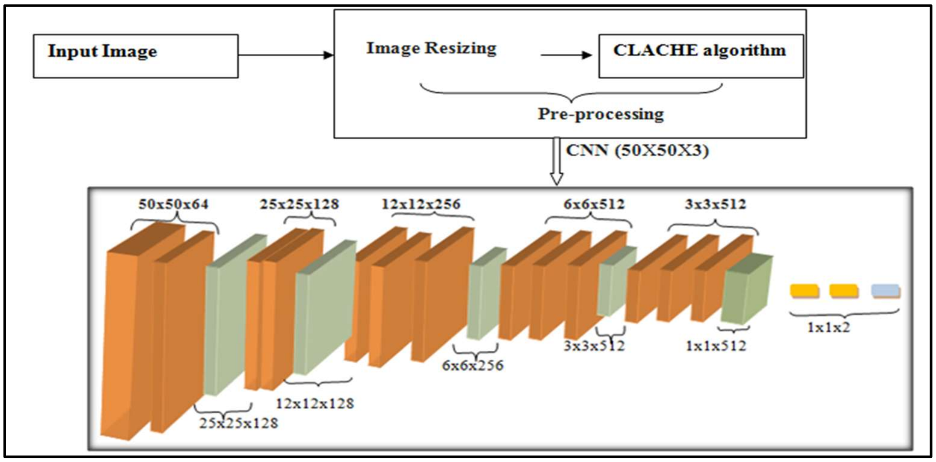


Fig. 9. A typical architecture of CLAHE-CNN

As shown in Fig. 9, initially pre-processing is done on raw images to increase classification performance. So the given input image is resized to a defined size i.e., 50 x 50 without changing image qualities. The resizing is done on images from various datasets such as IMD, GRIP, and MICC-F220. The CLAHE (Contrast Limited Adaptive Histogram Equalization) algorithm is utilized in the pre-processing step to enhance the visibility of hidden characteristics that may have been duplicated with noise and altered in color due to copy-move forgery. This algorithm employs histogram equalization after the image is partitioned into small blocks. To combine adjacent blocks and to remove the induced borders bilinear interpolation is used so that it prevents possible block artifacts among the blocks. To identify the forged regions, the CLAHE algorithm improves the contrast of an image to make the hidden information visible. A pre-processed image is given as input to the CNN model.

In this deep learning model, an input layer is followed by thirteen convolution layers in the CNN. Every layer had a ReLu activation function, with a 3 x 3 filter size, one stride, and one padding. To initialize the weights in the first convolution layer, 64 high-pass filters with sizes 3 x 3 x 3 are used. The weights of every layer are calculated according to the filter size and the number of filters used on a layer. In the softmax layer, to represent the categorical data one hot encoding is used. It is a vector with several components based on the number of classes present. In this algorithm, authentic images are identified as class 1 and forged images are as class 2. When the primary image is given as input for the network, it outputs the vector as [1,0] and [0,1] as output for forged images.

The performance of the dataset can be enhanced using Generative Adversarial Network. GAN creates a new version of image which is similar to original image. This GAN can be combined with CNN for the ease identification of copy-move forgery. This typical deep learning architecture is discussed.

5.3 Generative Adversarial Network (GAN) and Convolutional Neural Network (CNN) for copy-move forgery

The authors of [23] proposed two-branch architecture and a fusion model. This two-branch architecture is used to localize and detect the copy-move forgery using GAN and CNN. The methodology of GAN is simple – it is composed of two components namely Generator (G), and the Discriminator (D). The generator takes input as image (I) and generates a forged image (I') as an output I' = G (I) for the given image. The discriminator is trained to take, either the original image or generated image I' as input. The overview of this model architecture is [23] shown in

Fig. 10.

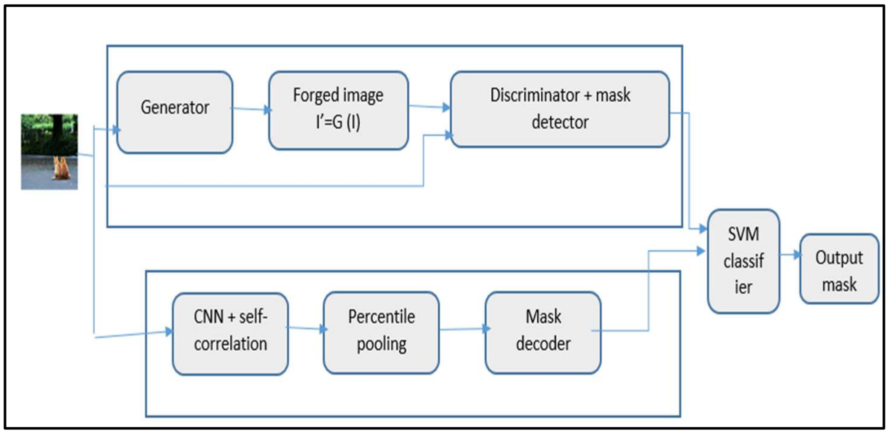


Fig. 10. A typical architecture of GAN and CNN model.

As shown in Fig. 10, the approach discussed in this sub-section consists of two models namely GAN and CNN. The upper part of the diagram represents the GAN model and the lower part represents the custom-CNN based model. These two models are trained as a game between the generator and discriminator. The purpose of generator is to create forged images for original images and they are difficult to identify. The generator network aims to change the d-dimensional noised vectors into 28 x28 images with the help of up-sampling. The job of the discriminator is to produce the correct classification of images which are manipulated by G. The discriminator used in this approach comprises six convolutional layers, seven ReLU layers, and two fully connected layers. The main aim of discriminator is used to identify and differentiate the accuracy between real patches and regenerated patches which are obtained from real and fake images. Apart from the above model, a custom CNN model is implemented to identify similar forged regions by performing the correlation operation on the input features, which are given as input for the mask detector. A mask detector gives the similarities across the target area and recasts the features to the actual size of an image. Finally, the Output of GAN model and custom CNN model outputs are combined to a single SVM classifier layer. In this layer, a linear classifier Support vector machines (SVM) [24] is applied to decide the authenticity of an image. This layer is helpful to localize the copy-move forgery, and gives distinction between the original image and forged image.

For the training task, the experiments were conducted on CIFAR [25], and MNIST [25] datasets. CIFAR dataset images are categorized into ten distinct classes. In contrast, MNIST consists of 28 x 28 grayscale images. Additional datasets such as MICC-F600 and IM dataset and Oxford datasets are considered for testing the performance of the given model. To yield the better results in localization of copy-move forgery, a unified architecture called Long short-term Memory (LSTM) can be used. It localizes the altered regions of an image. The enhanced version of LSTM i.e., ConvLSTM is discussed in section.

5.4 ConvLSTM for Copy move forgery

The authors of [26] proposed a model using deep learning with a hybrid modality of Convolutional Network Layer (CNN), and Convolutional Long Short-Term Memory (ConvLSTM). This model is implemented in three stages. As shown in Fig. 11, in the first stage, pre-processing is performed to unify the size of input images to a defined size and convert them into tensors. In the second stage, features are extracted from the input images using one convLSTM layer with 16 filters, and three convolution layers, followed by pooling layers. Different filters in sizes 32, 64, and 128 were applied on these three convolution layers and each convolution layer is followed by a pooling layer. The ConvLSTM model architecture is shown in

Fig. 11.

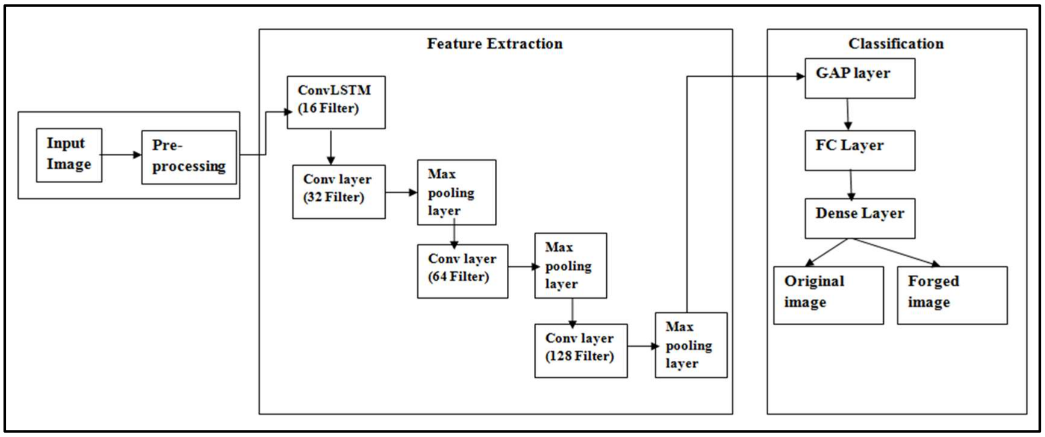


Fig. 11. Layered architecture of the ConvLSTMmodel

The sequence shown in the feature extraction module generates a feature map to represent the input image, and it becomes the input for the classification. In classification, the Global Average Pooling (GAP) layer and FC layer are combined, and they deal with feature maps. Finally, feature maps are converted into feature vectors.

LSTM is a special type of Recurrent Neural Network (RNN) used to handle sequential data and to remember the previous output. The problem with the LSTM structure is the existence of spatial data. To address this problem ConvLSTM is used. This ConvLSTM uses Conv layers in place of the FC layer in LSTM and the spatiotemporal information is encoded in its memory cell. Convolution layers shown in Fig. 11, consists of two-dimensional digital filters. These filters are initialized with some random weights and perform the feature extraction on the input images. In training process, the weights for these filters are updated. This process is used to generate the feature maps. The output of every layer is evaluated by Relu activation function. A pooling layer is used to reduce the dimensions of feature map generated at each convolution layer.

This model has been experimented on various datasets such as SATs-130, MICC-F2000, MICC-F600, and MICC-F220. To avoid over fitting problems because of small datasets, datasets are merged to build a new dataset and this dataset consists of 2916 images, among them 1010 are forged and 1906 are original images. The k-fold cross-validation technique is performed to assess this model. The authors used various evaluation metrics to evaluate the performance of the model such as TPR, TNR, FNR, FPR, and Accuracy.

The layered architecture of ConvLSTM model addressed the classification of an input image as original or as forged image but it did not perform the localization of the forged region in images. The authors didn’t train the model on different datasets like CASIA, Coverage, and CoMoFoD. All the discussed approaches not addressed the detection of forgery in small areas of an image or low-resolution images. To identify the copy-move forgery in low resolution images another deep learning architecture called Quality independent deep learning is discussed in section 5.5.

5.5 Quality Independent Deep Learning (QDL) based Copy-move Forgery

The authors of [27] proposed Quality Independent Deep Learning (QDL) based copy-move forgery model to detect the forgery in small areas, low-resolution images, and inferior images. As shown in Fig. 12, a reference less or blind quality assessment is performed on the given image to improve its quality before the forgery detection. It is performed with the help of GANs

[28]. To detect the copy-move forgery, dual branch CNN architecture is used which consists of two sub-networks. One is a manipulation detection sub-network which is used to perform the segmentation and it segments the altered regions in the image. The other is the similarity detection subnetwork to identify the similarities between the regions of an image. The composition of these two sub-networks generates forged and non-forged regions of an input image and also identifies the source and target of the forgery. The architecture of QDL-CMFD is shown in Fig. 12.

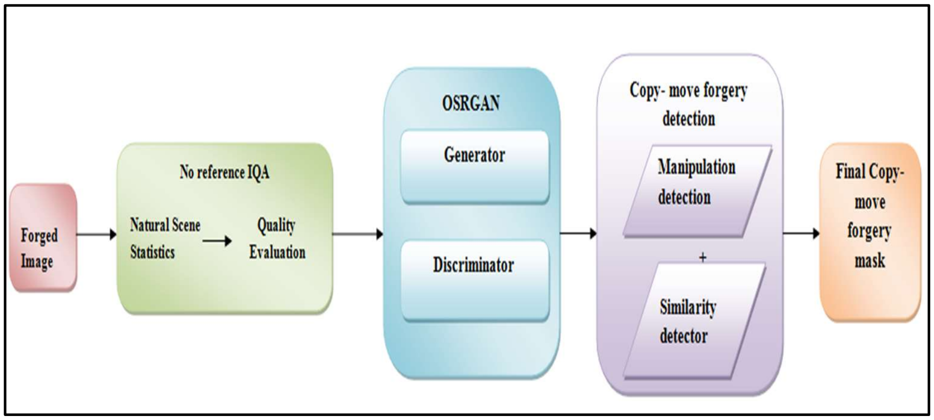


Fig. 12. QDL-CMFD architecture

To evaluate the quality of an image, a Blind or Reference less Image Spatial Quality Evaluator (BRISQUE) [29] is used. It also determines the images which are no longer natural because of distortions. Features are extracted using either the original image scale or the lower resolution of an image. A total of 36 features are used to evaluate the quality of an image. The quality score is mapped using an SVM [30] with Radial Basis Function (RBF) kernel. The quality score is normalized from 0 to 100. 100 represents the highest image quality. Images with low scores undergo with image enhancement process before the forgery detection. This enhancement process is implemented by an optimized version of Super-Resolution using GANs (SRGAN) [28] i.e, OSRGAN. OSRGAN model consists of two networks: 1. Generator network and 2. Discriminator network. A Generator network is used to produce the Super-resolution (SR) image as a counterpart for the given low-resolution image. The discriminator network is used to differentiate the Super-resolution and high-resolution (HR) images. Finally, the image is imported to two sub-networks of CNN to detect the copy-move forgery. Feature extraction is performed by using CNN. Feature similarity is calculated and statistics are measured by applying self-correlation and percentile pooling modules. Now the feature maps are expanded to the same size as the original image and a manipulation mask is produced.

6. Conclusion

In this paper, we provide a survey to detect the copy-move forgery and to localize the forged regions using deep learning approaches. The presented methods worked on several benchmark datasets and produced good results. We also listed different data sets and their details like the size of images, the format they support, number of original or forged images within the dataset which are widely used for common image forgery attacks like copy-move forgery and splicing attacks. We gave a overview of various deep learning approaches to perform the feature extraction and segmentation with ADM, discussed an approach to make the hidden the hidden patterns visible using CLAHE-CNN, an approach of GAN's and custom CNN models to localize and target the forged regions of source image, and etc. We also made comparisons between traditional approaches and deep learning approaches. We discussed performance of these approaches which work better in yielding good results for copy-move forgery attack and their limitations.

References:

1. Passarella A (2012) A survey on content-centric technologies for the current internet CDN and P2P solutions. ComputCommun 35(1):1–32. https://doi.org/10.1016/j.comcom.2011.10.005
2. Arnold MK, Schmucker M, Wolthusen SD (2003) Techniques and applications of digital watermarking and content protection. Artech House
3. Nikolaidis N, Pitas I (1996) Copyright protection of images using robust digital signatures. In: 1996 IEEE international conference on acoustics, speech, and signal processing conference proceedings, vol 4. IEEE, pp 2168–2171. https://doi.org/10.1109/ICASSP.1996.545849
4. Piva A (2013) An overview on image forensics. International Scholarly Research Notices 2013. https://doi.org/10.1155/2013/496701.
5. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y (2014) Generative adversarial networks. Adv Neural Inf Process Syst 3.
6. Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E (2012) An evaluation of popular copy-move forgery detection approaches. IEEE Trans Inf Forensics Secur7(6):1841–1854. https://doi.org/10.1109/ TIFS. 2012.2218597
7. Tralic D, Zupancic I, Grgic S, Grgic M (2013) Comofod — a new database for copy-move forgery detection. In: Proceedings ELMAR-2013, pp 49–54
8. Dong J, Wang W, Tan T (2013) Casia image tampering detection evaluation database. In: 2013 IEEE China summit and international conference on signal and information processing, pp 422–426. https://doi.org/10.1109/ChinaSIP.2013.6625374
9. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G (2011) A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans Inf Forensics Secur:1099–1110. https://doi.org/10.1109/TIFS.2011.2129512
10. Christlein V, Riess C, Angelopoulou E (2010) On rotation invariance in copy-move forgery detection. In: 2010 IEEE international workshop on information forensics and security, pp 1–6. https://doi.org/10.1109/WIFS.2010.5711472
11. Korus P, Huang J (2016) Evaluation of random field models in multi-modal unsupervised tampering localization. In:2016 IEEE international workshop on information forensics and security (WIFS), pp1– 6. https://doi.org/10.1109/WIFS.2016.7823898
12. Korus P, Huang J (2017) Multi-scale analysis strategies in prnu-based tampering localization. IEEE Trans Inf Forensic Secur
13. Navneet Kaur, Neeru Jindal, Kulbir Singh (2022) A deep learning framework for copy-move forgery detection in digital images Multimedia Tools and Applications https://doi.org/10.1007/s11042-022-14016-2
14. B. Mahdian, S. Saic, Detection of copy-move forgery using a method based on blur

moment invariants, Forensic Sci. Int. 171 (2007) 180–189.

15. D.G. Lowe, Distinctive image features from scale-invariant key points, International Journal of Computer Vision 60(2) (2004), 91–110.
16. S. Prasad and B. Ramkumar, Passive Copy-Move Forgery Detection using SIFT, HOG and SURF Features, IEEE International Conference on Recent Trends in Electronics Information Communication Technology, May 20-21, India, doi:10.1109/rteict.2016.7807915, 2016.
17. H. Bay, A. Ess, T. Tuytelaars, L. van Gool, Speeded Up Robust Features (SURF), Comput. Vis.ImageUnderst. 110(2008) 346-359.
18. Khurshid Asghar, Zulfiqar Habib, Muhammad Hussain, (2016) Copy-move and splicing image forgery detection and localization techniques: a review. Australian Journal of Forensic Sciences, http://dx.doi.org/10.1080/00450618.2016.1153711.
19. Ning X, Gong K, Li W, Zhang L, Bai X, Tian S (2020) Feature refinement and filter network for person re-identification. IEEE Trans Circuits Syst Video Technol 31:3391–3402
20. Ning X, Gong K, Li W, Zhang L (2021) JWSAA: joint weak saliency and attention aware for person re-identification. Neurocomputing 453:801–811.
21. Agarwal R, Verma O (2020) An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. Multimed Tools Appl 79. https://doi.org/10.1007/s11042-01908495-z
22. Achanta R, Shaji A, Smith K, Lucchi A, Fua P, Su¨sstrunk S (2010) Slicsuperpixels. Technical report, EPFL
23. Younis Abdalla, M. Tariq Iqbal, and Mohamed Shehata, Copy-Move Forgery Detection and Localization Using a Generative Adversarial Network and Convolutional Neural-Network, Information 10(09):286. https://doi.org/10.3390/info10090286
24. Bupe, C. Why Is SVM Not Popular Nowadays; University of Zambia: Lusaka, Zambia, 2018; Available online: https://www.quora.com/ (accessed on 25 April 2019).
25. Krizhevsky, A. Learning Multiple Layers of Features from Tiny Images; University of Toronto: Toronto, ON, Canada, 2009.
26. Mohamed A. Elaskily, Monagi H. Alkinani, Ahmed Sedik, and Mohamed M. Dessouky, Deep learning based algorithm (ConvLSTM) for Copy Move Forgery Detection. Journal of Intelligent & Fuzzy Systems 40 (2021) 4385–4405, DOI:10.3233/JIFS-201192.
27. Mehrad Aria, Mahdi Hashemzadeh, NacerFarajzadeh,(2022) QDL-CMFD: A Quality-independent and deep Learning-based Copy- Move image forgery detection method. pp 213-236. https://doi.org/10.1016/j.neucom.2022.09.017
28. C. Ledig, L. Theis, F. Huszár, J. aballero, A. Cunningham, A. Acosta, A. Aitken, A. Tejani, J. Totz, Z. Wang, Photo-realistic single image super-resolution using a generative adversarial network, Proc. IEEE Conf. Comput. Vision Pattern Recogn. (2017) 4681-4690.
29. A. Mittal, A.K. Moorthy, A.C. Bovik, No-reference image quality assessment in the spatial domain, IEEE Trans. Image Process. 21 (2012) 4695-4708.
30. B. Scholkopf, A.J. Smola, R.C. Williamson, P.L. Bartlett, New support vector algorithms, Neural Comput. 12 (2000) 1207–1245.

31. I. Amerini, L. Ballan, R. Caldelli, A.D. Bimbo and G. Serra, A SIFT-based forensic method for copy–move attack detection and transformation recovery, IEEE Transactions on Information Forensics and Security 6(3), Sep. 2011.