An intelligent system to detect and classify the image forgery attacks : copy-move forgery and image splicing

Riya Patel[1], Dr. Ravi Sheth[2], Mr. Jatin Patel[3]
[1]School of Information Technology, Artificial Intelligence and Cyber Security
Rashtriya Raksha University, Gandhinagar, Gujarat, India
[2]School of Information Technology, Artificial Intelligence and Cyber Security
Rashtriya Raksha University, Gandhinagar, Gujarat, India
[3]School of Information Technology, Artificial Intelligence and Cyber Security
Rashtriya Raksha University, Gandhinagar, Gujarat, India

Abstract: Image forgery means the malicious modification of digital images with the intention of fraud which hardly leaves any detectible traces to detect a forged image we need so much information about the image (for e.g.: RGB, Retouching, Resize, Checksum, file name, file creation date/time, etc).to gathering this type of image we use many tools like Winhex, Image processing, ExifTool, Adobe, etc. if any person wants all the information about the image then person wants to use many tools that take too much time and skillset in our case we show two attacks on image, copy- move forgery attack and image splicing attack. we check the original image and forged image information. Also, check the accuracy of the original image and forged image and create a report that shows the original image and forged image information. This will help layman and forensics investigators as well and will save time. We have seen images have played a major role as evidence in many crime scenes and this would create a major impact in investigation and forensics analysis. This tool could also help law enforcement agencies.

Keywords: Digital forensics, splicing attack, copy-move attack, chroma components, Discrete Cosine Transformation, Local Binary Pattern, Support Vector Machine.

1. Introduction

The rise of the digital world is changing our way of storing and processing data. Digital images, because of their ease of acquisition and storage, are the quickest means of knowledge transfer. These images can be used as evidence, such as the images seen in TV news can be recognized as proof of the veracity of that news. While this technology has many benefits, it can be used to conceal facts and evidence as well. Today, digital images are manipulated in such a way that the identification of forgery with naked eyes is not feasible. Forgery is the act of illicitly copying or reproducing documents, signatures, photographs or banknotes. The method of making fake images is forgery. With applications such as Adobe Photoshop, GIMP, and Corel Paint Store, forgery is easily possible. For malicious purposes, some forgers conduct the forgery to conceal important features of an image or to transmit some incorrect information by changing the text. In this scenario, the image's dignity and credibility are lost.

Techniques for detecting image forgery was divided into 2 groups.: - Active approach and Passive approach. [1] In the Active approach, Some pre-processing includes digital files, such as watermarking or digital signatures, etc. The method of inserting a digital watermark (a recognized authentication code) into the image on the source side is the Digital Watermarking technique, and then this code is used at the time of detection for digital information verification. Watermarks from the photos are inseparable. The drawback of the Watermarking method is that at the time of recording the image before dissemination by an approved individual with specialized cameras, it needs to be embedded in the image, but nowadays most of the cameras are not equipped with the watermark embedding feature. This can result in image deterioration as well. The Digital Signature method extracts and encodes the specific features of the image to generate digital signatures. At the time of detection, these signatures are used for authentication.

The passive approach is also referred to as the blind approach, which does not require any prior image knowledge. Image forensics is a passive approach that operates on the assumption that no visual traces are left by these forgeries; they which modify the image's statistical properties, referred to as image fingerprints, which define the image's life cycle from its acquisition to its processing. The distortion of the image distorts the fingerprints that produce image inconsistencies. In order to detect the tampered area, the passive method applies techniques for verifying these fingerprints. The location and amount of forgery in the picture is determined by the passive method. Passive approach has two methods:-

A. **Image source identification:-** This group concerns with the difficulties associated with the data source recognition. It checks whether the image is created by a computer or a natural image and also specifies the system that is used to acquire the image.

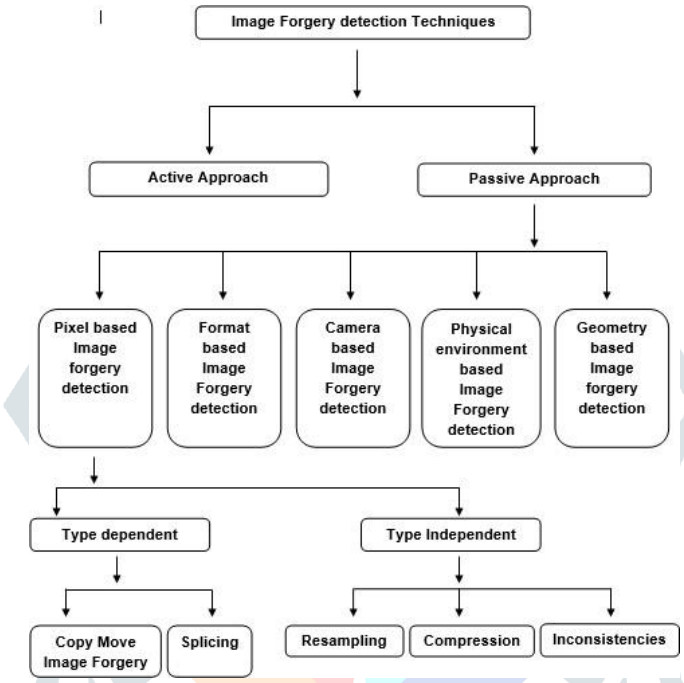
B. **Tampering detection:-** Owing to the availability of digital editing software, image manipulation has become much simpler, adding to the difficulty of forgery detection. It detects picture manipulation. Many basic operations, such as colors, contrast changes, brightness, and so on, can be used to detect image forgery. Suppression operations, such as filtering, compression, and noise extraction, can also be used to detect image forgery.

Passive approach can be further categorized:-

Pixel-based image forgery detection: Pixel-based approaches concentrate on the image pixels and identify statistical differences at the pixel level. The following approaches are further categorized: Image Resampling, Image Splicing, Copy-Move Falsification.

Format-based image forgery detection: In JPEG formats, Format based techniques are based on image formats and works mainly. in the compressed images, Format based techniques can detect forgery. JPEG Quantization, JPEG Blocking, and JPEG Compression are the three types of techniques.

Camera-based image forgery detection: When the image is taken by a digital camera, the image travels from the camera sensor to the memory. Four groups can be grouped into these techniques: Chromatic Aberration, Sensor Noise, Camera Response, Selection of Color Filters. There are a number of processing steps, including quantizing, white balance, filtering, compression of JPEG, etc. [1]



Physical environment-based image forgery detection: Consider the formation of an image by splicing two individual images taken at various locations together. Here, difficulty sometimes arises to match exactly the lighting effects originally photographed under each picture. As proof of forgery, these lightening variations can be used. Techniques based on the physical world function on the basis of a lightening environment. These techniques are categorized as: Light Direction 2-D, Light Environment, Light Direction3-D.

Geometry-based image forgery detection: Geometry-based approaches calculate real-world objects and their location in relation to the camera. Principal Point and Metric Measurements are two geometry-based approaches.

Pixel-based image forgery detection:-

Pixel based techniques are further categorized: Image Resampling, Image Splicing, and Copy-Move forgery

1. **Image Resampling: -** It is considered a less damaging form of forgery. Picture Resampling does not modify the image, but only decreases or enhances the image characteristics. This technique is most popular among photo editors of newspapers and magazines. This is not ethically proven to be wrong. It requires rescaling, resizing, image rotation etc.
2. **Image splicing: -** Image splicing is characterized as a paste- up created by photographic images sticking together. Image Splicing is a technique that involves the creation of a new fake image by composing two or more images. The splicing of photos is more offensive than there sampling.

Copy-Move forgery: - In order to mask details or alter the meaning of the image, it is the most common type of forgery technique in which one portion of the image is copied and pasted into various locations of the same image; therefore, there is a clear connection between these that can be used as proof to detect copy-move forgery. **Copy-Move Forgery challenges:**

- It is likely that the duplicated region is not the same original region. Any pre-processing can include it.
- Under Lossy Compression, images can be saved.
- In order to make forgery detection difficult, noise can be added to the image.
- A region may be rotated before forgery is performed.
- The area you copied could beblurred.
- The texture of a copied area may be altered. It can be colored darker or lighter.

Image Retouching

The method of changing an image to prepare it for the final display is photo retouching. Usually, retouchers execute acts that are small localized changes to an image. Retouching is the polishing of an image, typically completed following globalized changes (such as color correction). A retoucher will concentrate on changing other elements of an image once the white balance, cropping, and color profile have been established.

Image Retouching is carried out to improve the image characteristics. [1] Image on the Right side Fig 2 (b) has better color contrast than image on Left side. **Image Splicing:**

Fig 1: To create a new image by Splicing two individual images are used.

Copy move Forgery:

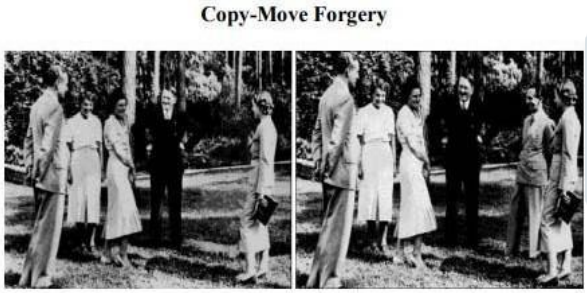


Fig 3(a) fig 3(b)

Image (a) in Fig 3 is the original image of only 5 people, and image (b) is a distorted image with 6 people standing in which one person is copied from the same picture and pasted into the same image at different locations. [1] **Copy move Forgery with Rotation:**

Fig 4(a) Fig 4(b)

In Fig 4, image (a) is the original image and image (b) is the tampered image in which rotation is performed on street lamp before copied and pasted. **Copy move Forgery with Scaling:**

Fig 5(a) fig 5(b)

Fig 5(a) is original image having 7 guns and Fig 5(b) is Tampered image in which Scaling is performed before copied and pasted.

The Copy-Move forgery detection can be categorized into two methods [1]:-

• Block based Methods

• Key point based Method

In this paper, We're using the Block Form. Centered on Discrete Cosine Transformation (DCT) and Local Binary Pattern (LBP) and a new feature extraction technique using the mean operator, the method was proposed. First, images are split into non-overlapping fixed-size blocks, and 2D block DCT is used to capture changes due to image forgery. Then, to improve forgery artifacts, LBP is added to the magnitude of the DCT collection. Finally, over all LBP blocks, the mean value of a given cell is computed, which yields a fixed number of features and provides a more computationally effective process. Using Support Vector Machine (SVM), On four well-known publicly accessible gray scale and color image forgery datasets, and also on an IoT-based image forgery dataset that we developed, the proposed method has been extensively tested. [2]

In every Image forgery detection method we can find accuracy for particular one techniques, models and datasets so here we create a system that supports two or more techniques , models and datasets.

Using this system we can save our time and improve accuracy.

in this paper, We implement a new technique of detection of image forgery and test it with comprehensive experimentation. [2]

2. Literature Review

This review paper establishes survey on various types of image forgery attacks including Copy Move Image Forgery and the Image Splicing.

In this paper [1] **(Copy-Move Forgery Attack Detection in Digital Images),** The numerous copy move forgery detection techniques that include Block-based & Key Point-based techniques were discussed. The system cannot detect Forgery in case of Overlapping, Compression, and Enhancement.

In this paper [2] **(A Robust Forgery Detection Method for Copy–Move and Splicing Attacks in Images)**, On four well-known publicly accessible gray scale and color image forgery datasets, and also on an IoT-based image forgery dataset they developed, the proposed method has been extensively tested. Experimental findings show the superiority of our proposed approach in terms of commonly used performance metrics and computational time over recent state-of-the-art methods and demonstrate robustness against the low availability of forged training samples. when the target image were in compressed(jpeg) format, the method was Struggled to cope with image scaling.

In this paper [3] **(Image forgery detection based on Gabor Wavelets and Local Phase Quantization),** This provides an innovative technique. This technique takes texture information of the image as a distinguishing feature. Here, Gabor wavelets and Local Phase Quantization (LPQ) are primary, extracting relevant texture characteristics that are fed for classification as input to a Support Vector Machine. On both CASIA v1 and the DVMM color dataset, the results display a precision of over 99 percent. [3] This method exceeds the performance of similar methods in solving image forgery detection. However, this method requires the higher dimension feature vector due to which it involves great amount of time and efforts in processing the image.

In this paper [4] **(Detecting Splicing and Copy-Move Attacks in Color Images),**There are two proposed methods in the detection of splicing and copy move attacks such as Discrete Cosine Transformation (DCT) and Local Binary Pattern (LBP). In terms of accuracy of detection, these methods show results of 97.52% in case of

Columbia Colour, 97.79% in case of CASIA-1 and 99.82% in case of CASIA-2. It should be noted that these methods have been tested on specific dataset(s) and have not been applied to all the data experiments. Accordingly, only the results of the specific data experiments are being determined.

In this paper [5] (DETECTING IMAGE SPLICING USING GEOMETRYINVARIANTS AND CAMERA CHARACTERISTICS CONSISTENCY),an authentic image and a spliced image are classified using semi-

automatic geometry invariants. To execute this action, firstly, the areas which may have been spliced are identified. Then, in each of the regions, geometry invariants are computed from the pixels. From each invariant, Camera Response Functions (CRF) are then estimated. Although this method has shown an accuracy level of 87%, it involves a substantial amount of time andefforts.

In this paper [6] **(Dual System for Copy-move Forgery Detection using Block-based LBP-HF and FWHT Features),** there are two block-based systems that are useful for copy-move forgery detection. One of the above is based on the extraction from the overlapping block and forgery decision of Local Binary Pattern Histogram Fourier characteristics based on the matching of these characteristics using Euclidean similarity calculation. The second is to extract Fast Walsh Hadamard Transform characteristics from each overlapping block and to decide on the matching of these characteristics using shift vector analysis. These two systems will be evaluated using irregular CoMoFoD dataset images.

In this paper [7] **(An Analysis of Image Forgery Detection Techniques),** There are tables that illustrate various types of methods for detecting image forgery. In this scenario, a bird's eye view of the information used to detect the forgery is also provided. However, for all the human interference pictures, this technique does not work. **In this paper** [8] **(Copy-Move Forgery Detection Using Segmentation),** The device makes parts of the image into tiny patches that are different. The method then extracts the characteristics in the picture and in the matching stage constructs a k-d tree. In addition, knn searches are performed on the patches to locate potential correspondence. The system records the patches where the number of

matching inlier points reaches a certain threshold of possible matching patches. The method depicts the copy-move region of the picture at the end of the process. The detection level, however, decreases where the .jpeg compression quality is low and more noise is added to the input image.

In this paper [9] **(An Efficiency Enhanced Cluster Expanding Block Algorithm for Copy-Move Forgery Detection),** This method improves previous cluster expanding block scheme to clustering by mean and variance to reduce the time. This method requires fewer computation time. However, the load of comparison increases as high as the number of datasets.

In this paper [10] **(Analysis of adversarial attacks against CNN-based image forgery detectors),** investigation is conducted in the aspect of how much effective adversarial attacks are on CNN-based detectors. A large set of manipulations and several CNN-based detectors are taken into consideration. To be precise, adversarial noise is generated for each detector. Then an assessment is held on the effects on the target detector and on non-target detectors. The performance of GAN-based restoration is also assessed. The considered detectors, false positive rate (FPR), true positive rate (TPR), and overall accuracy (ACC), in the absence of counter-forensic attacks. For easy cases (top), accuracies are always close to 100%. However, a somewhat worse performance, due to the limited training set is an exception to this. It is to be noted that the adversarial noise attack was not able to depict 7×7 median filtering, which closely modifies the image fine structures.

In this paper [11] **(Image Splicing Detection),** In order to demonstrate a proof-of-concept model, they intend to combine this new information with different pre-processing methods. They also shown the use of CNN and Autoencoder in the identification of image forgery. The proposed network would ideally be able to detect more meaningful and descriptive features through the use of residual learning than the handcrafted features used currently. A network of smaller than normal depth will retain more content from the original input and ideally allow for more meaningful associations between datapoint within both the CNN and the Autoencoder. A smaller network often benefits from a decrease in the size of the data set required for training and optimization to be accomplished. For the identification and localization of image forgery, the proposed residual CNN will be combined with an Autoencoder.

In this paper [12] **(IMAGE SPLICING FORGERY DETECTION),** In particular, image splicing forgery detection techniques address the detection of image forgery and various forgery detection techniques. To detect image composition, we have reviewed several methods proposed in research papers to emphasize the need for image splicing detection. This field is still growing and a lot of research is needed to make it more promising for digital forensics.

In this paper [13] **(Image Forgery and it's Detection Technique: A Review),** they have worked on DCT algorithm and analyse the method. The proposed system detect a forgery in image datasets with good success rate. The most widely used approach to detect duplication in the picture is the block matching algorithm or block tiling algorithm. The time complexity of such algorithms is one of the major challenges. This problem has been discussed in the proposed method(paper) without sacrificing the method's consistency. To reflect the characteristics of overlapping blocks, the Discrete Cosine Transform (DCT) is used.

Technique Proposed By	Publication Year	Features Extracted	Classifier Used	Dataset Used	Accuracy Rate As Claimed(%)	Limitation
Prinkle Rani Er. Jyoti Rani	2015	DCT, LBP	blocked based,	-	-	The existing system cannot detect forgery in case of overlapping, Compression & Enhancement.

Mohammad Manzurul Islam, GourKarmakar, JoarderKamruzzaman, ManzurMurshed	2020	DCT, LBP	SVM ,blocked based	Columbia-Gray, Columbia-color, CASIA-1, CASIA-2. Developed:FBDDF	Similar to nonscaled Images	Struggled to cope with image scaling when the target image were in compressed(jpeg) format.
Meera Mary Isaaca, M Wilscy	2015	Gabour Wavelets Local Phase Quantization	SVM	CASIA TIDE v1,DVMM	99.83 %	Large dimensionality of the feature vector which leads to a larger processing time.

Mohammad ManzurulIslam ,GourKarmakar, JoarderKamruzzaman ,ManzurMurshed ,GayanKahandawa	2018	LBP, DCT, Block Division of Input, Chroma Component	SVM with RBF	Columbia, CASIA, CASIA 2	Columbia:97.52 % CASIA :97.78 % CASIA 2:99.81%	Not All Works have experimented.
Yu-Feng Hsu, Shih-Fu Chang	2006	CRF using Geometric Invariants(Cross Fitting)	SVM	Canon G3, Adobe Photoshop,	87.55 %	Time Consuming
Badal Soni, Pradip K. Das, Dalton Meitei Thounaoja m	2017	LBP,LBP-HF,FWHT	Block based System	CoMoFoD	-	Not for Geometric Transformation attack.

Chandande ep Kaur, Navdeep Kanwal	2019	DCT, DWT, PHT ,PCT	SVD	MICC-F2000, MICC-F220, MICC-F600, CoMoFoD	-	Not Work for all Human intervention Images.
Bhavya Bhanu M P	2017	Constructs a k-d tree,theKnn(k-nearest neighbour search is performed on the patches), SIFT & SURE Key Points	Segmentation	-	-	Detection becomes less when quality of .jpeg compression is law & when more amount of noise is added to the input image.
Cheng-Shian Lin, ChienChang Chen, Yi-Cheng Chang	2017	Mean ,Variance key point	Block algorithm	MATLAB 7.11	-	Large number of Dataset increase the Comparison load.
Diego Gragnaniello, Francesco Marra, Giovanni Poggi, Luisa Verdoliva	2018	SPAM ,SRM	CNN	-	Close to 100%	The adversarial noise attackw as not able to conceal 7*7 median filtering.
Ryan Griebenow	2017	-	CNN	-	-	Not checked the dataset is capable of stateof-theart performance or not?.

SIDDHI GAUR, SHAMIK TIWARI	2017	-	-	-	-	a lot of research is needed to make Digital forensic more promising.
Varsha Sharma, Swati Jha , Dr. Rajendra Kumar Bharti	2016	DCT	Block based	-	-	Not accurate result

3. Conclusion

In this paper, We implemented an effective and robust model using conventional machine learning technique (SVM) and hand-crafted characteristics to detect splicing and copy-move attacks in both grayscale and color images. Experimental results in terms of detection accuracy and CPU time on different publicly available datasets and our newly developed techniques of forgery dataset confirm the superiority and robustness of our proposed method over existing methods found in the current literature. Results also show that our proposed method is more effective and consistent in detecting splicing and copy–move image forgery attacks even for a very low amount of forgery images in the training set. In the future, We will investigate the efficiency of forgery detection techniques based on deep learning. For such distortion, the forgery detection accuracy of our system can differ slightly. In our additional studies, we will also examine the effect of barrel distortion on forgery detection.

4.References

[1] P. Rani, "Copy-Move Forgery Attack Detection in Digital Images," *https://www.ijert.org/*, p. 7, 2015.

[2] M. M. Islam, "A Robust Forgery Detection Method for Copy–Move and Splicing Attacks in Images," *www.mdpi.com*, p. 22, 2020.

[3] M. M. Isaac, " Image forgery detection based on Gabor Wavelets and Local Phase Quantization," *www.sciencedirect.com*, p. 8, 2015.

[4] M. M. Islam, "Detecting Splicing and Copy-Move Attacks in," *www.researchgate.net*, p. 8, 2018.

[5] Y. H. a. S. Chang, "DETECTING IMAGE SPLICING USING GEOMETRY INVARIANTS AND CAMERA CHARACTERISTICS CONSISTENCY," *www.ee.columbia.edu*, p. 4, 2006.

[6] B. Soni, "Dual System for Copy-move Forgery Detection using Block-based LBP-HF and FWHT Features," *www.researchgate.net*, p. 11, 2018.

[7] C. Kaur, "An Analysis of Image Forgery Detection Techniques," *www.researchgate.net*, p. 16, 2019.

[8] B. B. M. P, "Copy-Move Forgery Detection Using Segmentation," *ieeexplore.ieee.org*, p. 5, 2017.

[9] C.-S. Lin, "An efficiency enhanced cluster expanding block algorithm for copy-move forgery detection," *www.researchgate.net*, p. 4, 2017.

[10] D. Gragnaniello, "Analysis of adversarial attacks against CNN-based image forgery detectors," *https://arxiv.org/*, p. 5, 2018.

[11] R. Griebenow, "Image Splicing Detection," *https://www.semanticscholar.org/*, p. 7, 2017.

[12] S. GAUR, "IMAGE SPLICING FORGERY DETECTION," *https://www.semanticscholar.org/*, p. 5, 2017.

[13] V. Sharma, "Image Forgery and it's Detection Technique: A Review," *https://www.irjet.net/*, p. 7, 2016.