Copy-Move Image Forgery Detection using Adhoc Algorithm

Prathyakshini

Abstract*: It is easy make fake images by making use of editing software. It has become an effortless job to put together or detach some attributes from an image. Validation of digital images is very essential. Identifying the fake image is the crucial topic. In order to identify tampered image active and passive detection methods are used. An image can be tampered by using image splicing, copy-move, and retouching. In particular, copy-move attack is considered in this paper. It is essential to find out whether the image is tampered or not. An effective method for detecting forged image is proposed which uses adhoc algorithm. In this algorithm there is no need of original image as it compares the similar pixels in the given image. Clusters which are larger than block size are pulled out. Similar clusters are extracted using some similarity function. The method successfully detects the forged parts in the image and saves the forged image in JPEG format. The performance is measured on various images.

Keywords: forgery detection, copy-move, image splicing, retouching, adhoc algorithm

I. INTRODUCTION

With the emergence of social networking services such as Whatsapp, Face book and Instagram there is increase in large amount of image data. The forged images are generated by making use of some editing software. A large number of top photo editing tools are available like Adobe Light room, Adobe Photoshop, skylum luminar and many more. There is also possibility of creating composite image by making use of different images. Many times images are downloaded from the internet and reused without getting any permission. The images are altered by adding or removing some features and they have used as evidence. A typical method is used to block reusing the image through digital watermarking. Digital watermarking places some information such as owner name or logo in to a digital media [1]. By using digital watermarking method, we can tell the data is used illegally without the owner's permission and proof for the same can be provided. There is also software available to add a proof of ownership to the images such as SignMyImage, Ice mark. Retouching the image can be done by refining the image in order to modify the look as shown in fig 1. There are lot many changes when original and tampered images are compared. An old man can look young by just removing wrinkles on his face. Splicing is another kind of image tampering technique where some regions in the image is modified by adding some objects from other sources as shown in fig 2. It is even possible that background of a picture can be modified by photos and shares it through social networking sites. However they enjoy receiving positive comments about their photos. Now a day there is an advanced feature which is directly available on the smart phone even without additional software image retouching can be done. For image validation many methods have been proposed. Image validation methods are designated as passive and active authentication. Facts about the image are a perquisite for active authentication. At the time of image generation some code snippet is placed into the image verifying the same code validates the originality of the image. Unlike active methods details about the image is not required. It uses image itself to check the image is tampered or not. In particular, copy-move attack is considered in this paper. In copy-move attack identical version of the image is created by attaching more features of the same image as depicted in figure 3. There may be an intension to cover the part of the image with some other segments. By comparing the forged image with the real one can easily detect forged region easily.

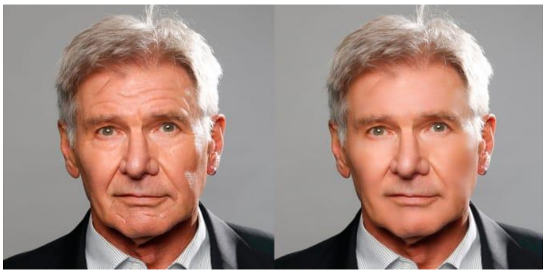

Fig. 1. Retouching done on right side image

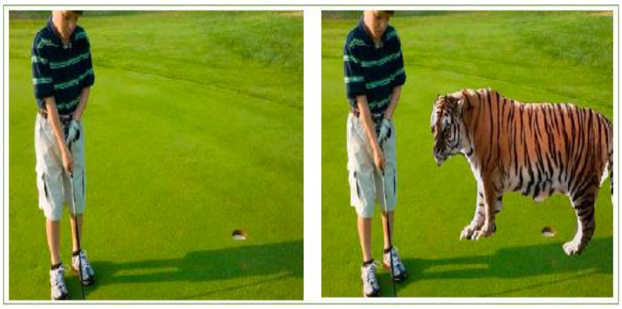

Fig. 2.Image splicing seen on the right image

Manuscript published on January 30, 2020.
* Correspondence Author

Prathyakshini*, Dept of Information Science and engineering, prathyakshini@nitte.edu.in

Example for a tampered image is shown in **fig 4** where the number of objects is more compared to the original one. Finding out changes in the image through analytical properties is not attainable for a human eye.

The forged region is identified by similar vector features. Finding greater level of entropy image area is the main idea in key-point based technique. From each key point a feature vector can be drawn out. As the number of key point is reduced less number of feature vectors is estimated.

II. LITERATURE SURVEY

A new deep neural network is proposed by Yue Wu, et.al [2] where copied parts were detected successfully. In order to draw out the block like features a neural network was used. Matched points were localized by using point-wise feature extractor. It was shown that the results obtained were highly efficient compared to previous results. Jessica Fridrich et.al [3] proposed an efficient and reliable approach to find out tampered image. The forged area was successfully detected even in case of enhanced image. The method was demonstrated on several images. Parul sharma, Harpreet Kaur [4] proposed GLCM (Gray Level Co-occurrence Matrix) and Euclidian Distance Technique for detecting tampered image.

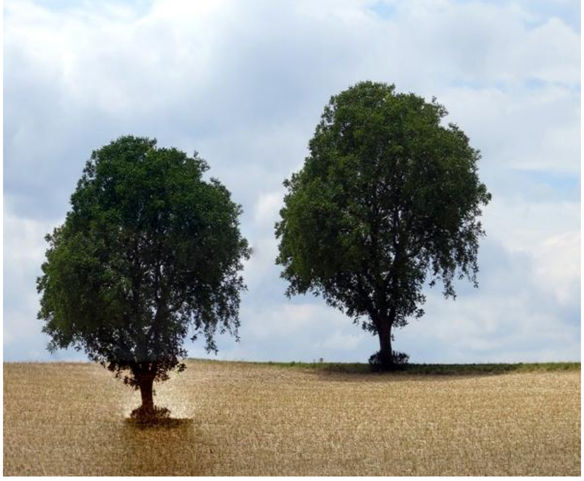

Fig. 3.Example of Copy-move attack on image

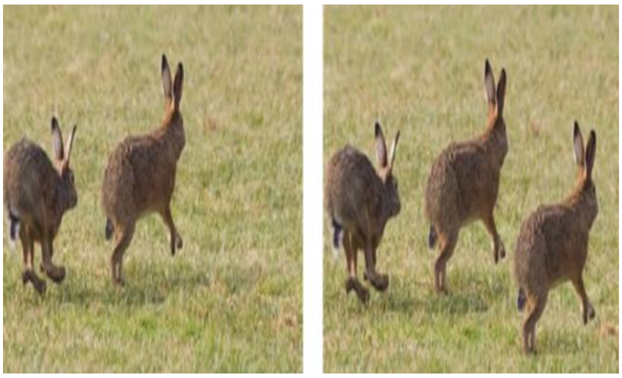

Fig. 4.Additional object seen on right image

The forgery detection was carried out based on feature extraction, Euclidian distance and image marking steps. For forgery part detection Euclidian distance is calculated. For Feature extraction GLCM is used. Mat lab simulator was used to implement this proposed technique.

Different parametric values are used analyze the proposed technique. Huan Wang and Hongxia Wang [5] proposed efficient method to detect the tampered image. Based on package clustering and perceptual hashing algorithms duplicate regions were found. The detection precision was improved by using package clustering algorithm. Younis Abdalla et.al proposed Convolution Neural-Network for identying tampered [6]. To find the suspicious image, an adversarial model and deep convolution model are used. A high performance was shown by deep learning CNN. A two Step Search Algorithm was proposed by Yong-Dal Shin [7]. In this method 96.82% computational complexity was reduced. None of the any exhaustive search procedure and frequency domain was used in sequence to lower the computational complexity. In this two step search algorithm, 2 pixels checking points were sufficient rather than 64 pixels checking points in the no tampered image region. A Hybrid Method for identifying fake images was proposed by Sunil Kumar et.al [8]. With different methods for key-point detection a hybrid method is proposed. In order to detect the key point SURF method is used and also for describing features of key point BRISK features are used. The proposed sytem is robust enough to affine transformation such as scaling and rotation.

III. PROPOSED TECHNIQUE

Adhoc algorithm is used to identify the tampered image. In this algorithm there is no need of original image as it compares the similar pixels in the tampered image. The block diagram for the proposed technique is depicted in Fig. 5. The proposed algorithm is robust enough to detect forgeries in lossy image format such as JPEG. There is also possibility that some objects are hidden and some are there are some various steps followed under this robust forgery detection algorithm. The algorithm is tested against the tampered images with copy-move image forgery. Also the original images were also given as input for validating the algorithm.

A. Proposed Algorithm Steps:

1. Convert the image into palette.
2. Break down the image into tiny M x M pixel blocks
3. Alphabetically oder the blocks using pixel value
4. Adjacent blocks with small definite color difference is drawn out
5. Find the intersection area of the blocks
6. Clusters which are larger than block size are pulled out.
7. Similar clusters are extracted using some similarity function
8. The discovered similar clusters on the images are drawn

The images in the format of PNG can use a palette. This Palette image is nothing but a table of 256 colors to enable better compression. Here 8 bit index is used to represent the position inside the palette and the color. Smaller footmarks palette image has both performance and cost benefit.

The experiment was carried on the Ubuntu platform using python 2.6.

The code was run using some default parameters by passing a sample image as an input. The block color deviation threshold value was lowered and the results were verified. There is a possibility that the input image is not tampered.

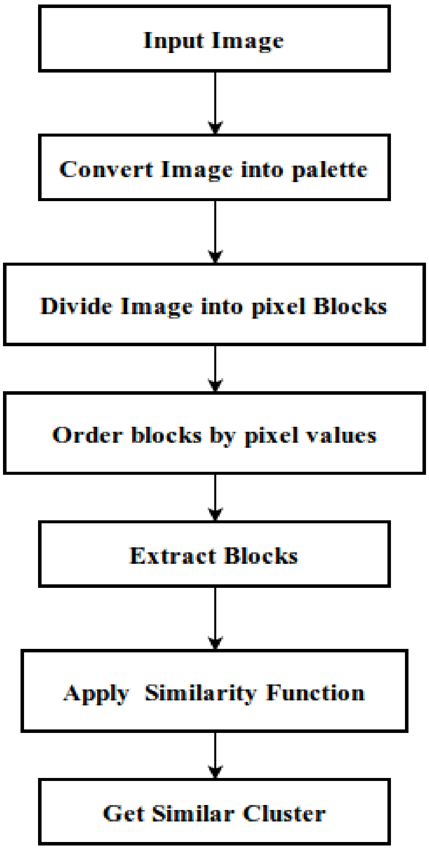
Input Image
Convert Image into palette
Divide Image into pixel Blocks
Order blocks by pixel values
Extract Blocks
Apply Similarity Function
Get Similar Cluster

Fig. 5.Block diagram of proposed system

IV. RESULTS

Several images were tested against the proposed technique. In this algorithm there is no need to compare the true image with the tampered one. Any format of the image can be taken like JPEG, PNG, and JPG. One of the types of copy-move attack is creating more amounts of objects in the image. Fig 6 shows the original image of this type of forgery. Fig 7 is a tampered image where objects are redundant. The cloning tank in the first row is detected as shown in Fig 8, but it is not detected in the following rows. This is because the tank is on the boundary of the image and it is very small. Different images were tested against the proposed algorithm. The proposed technique has better performance of image forgery detection. The following metrics are analyzed [9].

A. Accuracy

Accuracy is calculated as the ratio of true predicted instances to the total number of instances. A true positive is an exact prediction by the model where as true negative is a true prediction of negative class. False positive is a wrong prediction by the model where as false negative is a faulty prediction of negative class.

$$Accuracy(\%) = \frac{(TN+TP)}{(TN+TP+FN+FP)} \qquad (1)$$

B. Sensitivity

It is the degree of proportion of actual positive that are properly recognized.

$$Sensitivity(\%) = \frac{TP}{TP+FN} \qquad (2)$$

C. Specificity

It is the measure of proportion of actual positive that are precisely recognized.

$$Specificity(\%) = \frac{TN}{(TN+FP)} \qquad (3)$$

Pixel based metric needs true images which not provided by inference. Pixel of an image can be in either of 2 classes i.e. copy move or authentic. At each point there is a real output and estimated output. The result can be assigned to four metrics which are indexed using the confusion matrix as depicted in table1. Results were analyzed according to number of forged and true images as depicted in Table 2. FPR and FNR percentages determine how many true images are detected false and how many forged images are detected as true images. The results of the proposed technique are shown in Table 3. According to the image and image size the detection time and correct detection ratio is determined. Images with various sizes are considered here. Image correct detection gives percentage of detection for each image. By this overall accuracy can be determined

Table 1: Confusion Matrix

		Predicted (detection map)	
		Positive (copy-move pixels)	Negative (Authentic pixels)
Actual	Positive (copy-move pixels)	TP	FN
	Negative (Authentic pixels)	FP	TN

Table 2: Result obtained according to number of images

Forged Images	Unique Images	Sensitivity	Specificity	Accuracy	False Positive Rate	False Negative Rate
40	40	98%	96%	98%	8%	4%

Table 3: Results of proposed technique

Forged Image Name	Image Size in pixel	Detection Time (sec)	Correct Detection Ratio
beach.jpeg	1007×1520	0.54	100
cat.jpeg	1296×1944	0.81	92.74
giraffe.jpeg	1007×1520	0.54	96.25
tree.png	1224×1632	0.31	95.83
lighthuse.png	1007×1520	0.9	99.27
set.jpeg	480×640	0.18	100
sails.jpeg	1007×1520	0.8	99.27
horse.jpeg	1296×1944	1.3	100
cattle_copy.jepg	3039×2014	1.36	99.3
knight_moves2.jpeg	1007×1520	0.9	100

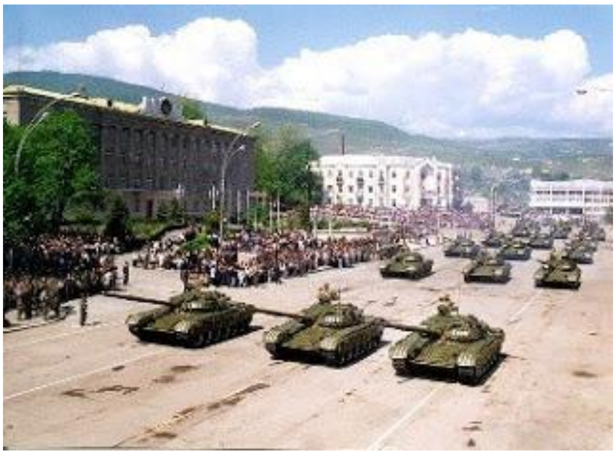

Fig. 6.True Image

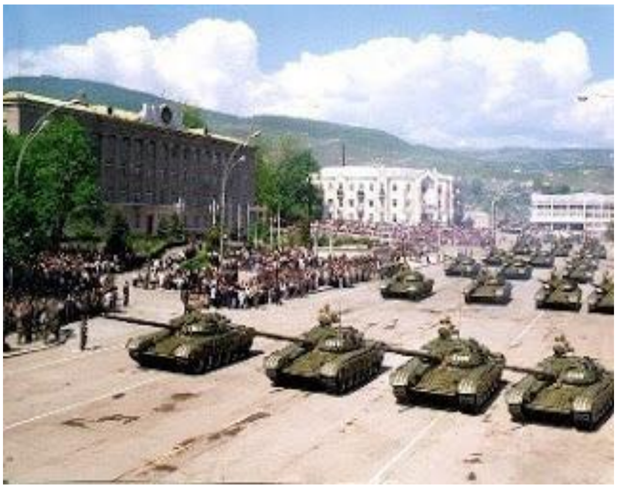

Fig. 7.Altered Image

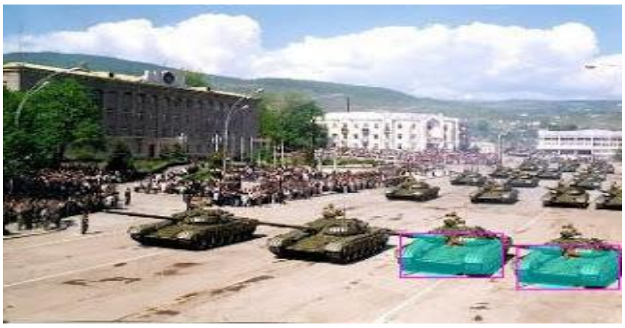

Fig. 8.Identification of Tampered Region

It is equally important to test images with forgery also images without any kind of forgery in it. Images with tampering can be tested against proper detection as well false detection. Similarly even original images without tampering can be verified against correct detection and false detection. By this algorithm efficiency can be checked. Sometimes some parts in the image may be hidden using some other parts of the same image this is also one of the tampering that comes under copy move forgery. If testing is considered then image size plays a wide role. When similar sizes of images are tested against this algorithm it takes comparatively less time. But when images of larger size are used, it consumes more time to show the result. Probably this issue could be addressed in future work.

V.CONCLUSION

It is simple and easy to create fake images out of available true images. There are types of methods exist to alter the images, copy–move approach is one of them. In copy-move attack identitical version of the image is created by attaching more features of the same image. This paper introduced an efficient method to identify the tampered region in digital images. An adhoc algorithm is used for this purpose. This is a pixel based detection of fake images. The algorithm is tested against several images and it has shown considerable improvement in the performance. The performance is measured using accuracy, sensitivity and specificity metrics. When similar sizes of images are tested against this algorithm it takes comparatively less time. But when images of larger size are used, it consumes more time to show the result. Probably this issue could be addressed in future work.

REFERENCES

1. Jobin Abraham,"Digital Image Watermarking: An Overview", National Seminar on Modern Trends in EC&SP, 3- 4 February 2011.
2. Yue Wu, Wael Abd-Almageed and Prem Natarajan, "BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization", 2018.
3. Jessica Fridrich, David Soukal, and Jan Lukáš, "Detection of Copy-Move Forgery in Digital Images", in Proceedings of the Digital Forensic Research Workshop, Cleveland, OH, USA, 6–8 August 2003.
4. Parul sharma, Harpreet Kaur, "Copy-Move Forgery Detection with GLCM and Euclidian Distance Technique in Image Processing", International Journal of Recent Technology and Engineering (IJRTE), Volume-8, Issue- 1C2, May 2019.
5. Huan Wang and Hongxia Wang, "Perceptual Hashing-Based Image Copy-Move Forgery Detection", Security and Communication Networks, 2018.

6. Younis Abdalla, M. Tariq Iqbal and Mohamed Shehata, "Copy-Move Forgery Detection and Localization Using a Generative Adversarial Network and Convolutional Neural-Network",mdpi,16 September 2019.
7. Yong-Dal Shin, "Fast Detection of Copy-Move Forgery Image using Two Step Search Algorithm", International Journal of Security and Its Applications Vol. 10, pp.203-214, 2016.
8. Sunil Kumar, J. V. Desai and Shaktidev Mukherjee, "A Fast Keypoint Based Hybrid Method for Copy Move Forgery Detection", International Journal of Computing and Digital Systems April 2015.
9. G. Clara Shanthi1 , V. Cyril Raj, "A Novel Approach for Efficient Forgery Image Detection Using Hybrid Feature Extraction and Classification", International Journal of Engineering & Technology, 2018.
10. Osamah M. Al-Qershi and Bee Ee Khoo, "Evaluation of Copy-Move Forgery Detection: Datasets and Evaluation Metrics", July 2018.
11. Rohini.A.Maind, Alka Khade, D.K.Chitre, "Image Copy Move Forgery Detection using Block Representing Method", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-2, May 2014.
12. Mohd Dilshad Ansari, S. P. Ghrera & Vipin Tyagi, "Pixel-Based Image Forgery Detection: A Review", IETE Journal of Education, 07 Aug 2014.
13. Gonapalli Ramu, S.B.G. Thilak Babu, "Image forgery detection for high resolution images using SIFT and RANSAC algorithm", Proceedings of the 2nd International Conference on Communication and Electronics Systems, Compliant, IEEE Xplore, 2017.

AUTHORS PROFILE

Ms. Prathyakshini, is an Assistant Professor in Information Science and Engineering department at NMAM Institute of Technology, Nitte. She has completed her M Tech in Computer Science & Engineering at SCEM, Adyar. She is an active member in ISSE. She has attended many workshops in image processing area. She has also conducted few technical workshops at NMAMIT, Nitte. She has published one international conference Scopus paper on "clustering of infested plant leaf using image processing. Her area of interest is image processing, machine learning.