A Survey on Image Forgery Detection Techniques

VandanaSangwan
Department of Computer Engineering
Punjabi University, Patiala
svandana08@gmail.com

MadanLal
Department of Computer Engineering
Punjabi University, Patiala
mlpbiuni@gmail.com

Abstract *–In today's technological era, digital images are the most common form of conveying information over internet, in journals, in newspapers, magazines, etc. To capture, create or modify/edit images has become very simple with the means of image processing and editing tools. Digital images are considered as proofs against various crimes or evidences for various purposes, so accuracy in digital images is very crucial but authenticating the tampered images is a major problem in the field of forensics, medical sciences. Basically copy-move forgery is one of the types of digital image forgery in which one region is copied and pasted into the same image or some other image with an intention to hide something or showing the scene which is not true. In this paper various techniques used to detect copy-move forgery are discussed.*

Keywords:Digital *Image forgery, Image Tampering, Copy-move forgery, DCT, JPEG images.*

I. INTRODUCTION

Nowadays, digital images are mostly used in every field. Digital images form the basic building block of every newspaper, journal, magazine, medical imaging, forensics, research field. But the security of digital images has become the biggest question if the images are tampered for malicious use. Image forgery is related somewhat to show in reality which is not true. For example, fig.1(a) showing original image whereas fig.1(b) shows two which is forged image i.e. content is copied from one image and pasted into same image to get new image.

Digital image forgery detection techniques are classified into two categories. One is active forgery. In active forgery, preprocessing operations are involvedfor example watermarking and signatures. In watermarking, a special symbol is hidden behind the content of image for maintaining its authenticity.

Fig.1(a)Original photoFig.1(b) forged photo

If the image is not manipulated then the watermark will remain same else image is not real. And in signatures, a visible signature is added to the image which is uniquely identifying it. Second is passive forgery, in which no pre-calculations are required and it is one of the difficult forgeries to detect. Image retouching, image splicing and Copy-move forgery comes under passive approach.In image retouching operations such as rotation, rescaling, contrast enhancement are performed. And in image splicing, two or more images are considered from which region is copied to form new image. Copy-move forgery is copying one region from an image and pasted in some other region.

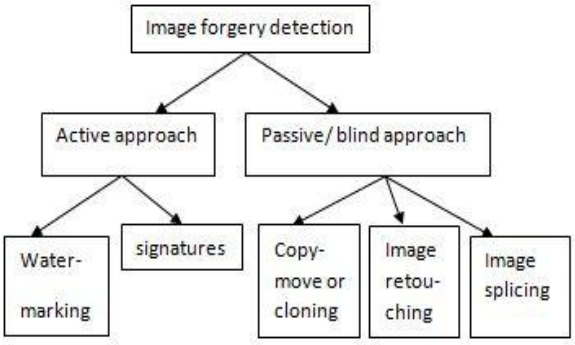

Fig.2 Basic forgery detection approaches

The structure of the paper is as follows: Section 2 elaborates thebasic technique and next sectionpresents review of literature.Then brief description in tabular formof techniques is given followed by the conclusion in section 4.

II. COPY-MOVE FORGERY

In copy-move forgery, one region is copied from an image and pasted onto other region of same image. It is also called cloning, when only one image is considered for forging process. In this the basic characteristics of the image remain similar such as texture, brightness, etc. Another copy-move forgery through composition is copying and pasting areas from one or more images and pasting onto an image being forged. This is called composite image forgery. It is very difficult to detect as the image sources are heterogeneous. Copy-move forgery manipulates both, image statistics and image content as well. Copying of regions may be done using some preprocessing operations such as rotation, rescaling, contrast enhancement which makes its detection hard.

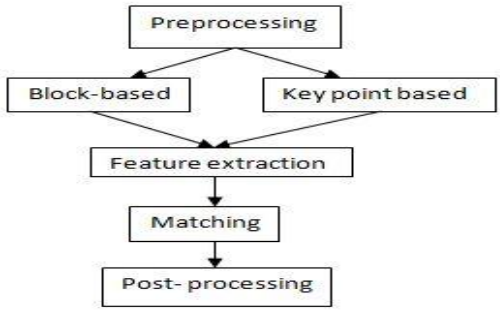

Fig.3Copy-move forgery detection basic pipeline stages.

The copy move forgery detection (CMFD) can classify into either Key-point-based methods or block based methods as shown above in Fig.3. In following section, we will discuss the techniques in frequency domain under copy-move forgery and will present a comparison in next section of those discussed techniques.

III. RELATED WORK

In this section, we have reviewed the passive methods for detection of copy-move forgery.MohammadFarukhHashmia, Vijay Anand, Avinas G. Keskar[1] presented a methodology using un-decimated wavelet transform in combination with SIFT which ensures better detection rates after preprocessing and other attacks. First the image is converted to wavelet form(DyWT) and then SIFT is applied to obtain the multispectral components and feature vector descriptors. Finally, go for finding the match between these feature descriptor vectors to mark the forged regions.

Ms. P. G.Gomase, Ms. N. R.Wankhade[2]proposed a technique in which DWT is applied to find the local changes in intensity in the image. Then median filter is applied to remove the noise, sets the values of every pixel to an average value. Then for detection process, divide image into blocks, and overlapping of those blocks to locate the copy-

move regions by pixel matching is done. This method is useful when images are preprocessed.

Ashima Gupta, NisheethSaxena, S.K Vasistha[3] proposed technique that can detect JPEG images using DCT coefficients to examine the double quantization effect. Here, detection is done by dividing the image into blocks then DCT is applied for fast computation and sorting it lexicographically then discarded those values whose threshold is higher and colored the pixels which are duplicated.

Muhammad Hussain, GhulamMuhammada,Sahar Q. Saleh, Anwar M. Mirza, and George Bebis[4] proposed a multiresolutionWeber local descriptor system which uses weber law to get image features. Firstly the colored image is changed into YCbCr color mode that stores the color components in chrominance and luminance factors. Then these components along with WLD are used to get the texture of the image. The histograms are plotted depending upon neighboring pixel values and those variations of histograms are concatenated & plotted to get the features. Then in last step, SVM classifier is used to classify the image as real or fake.

B.L.Shivakumar and Lt. S.SanthoshBaboo[5] described a system based on SURF(speeded-up robust features) algorithm to extract the features alongwith KD-tree to identify the forged region. In the first step SURF algorithm is applied over the image to extract set of key points with their corresponding SURF descriptors. Then a matching operation is carried out to identify the similar local patterns in the image. The best match is found for each keypoint by calculating Euclidean distance, later on KD-tree is used for searching nearest neighbors to detect duplicated regions. This method showed that it results in minimum false rate to detect forgery for images of high resolution.

P. Subathra, A. Baskarand D. Senthil Kumar[6] proposed technique based on resampling criteria using automatic selection of region of interest to find authenticity of images. The re-sampling process involves changing of original image into a new sampling lattice using some form of interpolation which introduces specific correlations into the image, and when detected can be used as proof of digital tampering. First of all, image is segmented to segment various objects using algorithms namely, K-means, watershed, etc. followed by dilation & erosion to smoothen the image. Then centroid is selected for given segmented object as region of interest, later the probability map containing periodic patterns is estimated and median filter is applied to remove additive noise from the image and FFT is calculated to detect the resampling patterns or duplicacy. This method helps to detect the preprocessed images but unable to detect if the image is converted to some other format.

S.DeviMahalakshmi, K.Vijayalakshmi,S.Priyadarshini[7] proposed a methodology for detecting manipulations which are done to forge the images using basic operations such as re-sampling(rotation, rescaling), contrast enhancement and histogram equalization. The detection of rotation/resampling is followed by preprocessing operation which includes changing image into YCbCr color mode. Then edge-map is generated by convolving (Y) component with laplacianoperator. Then DFT is calculated using DA and AD methods. The horizontal spectra obtained from DFT methods are plotted separately which shows peaks in it, and peaks are results of interpolation. It dictates that when an image is re-sampled, interpolation will take place. Secondly, for contrast enhancement and local histogram equalization, intrinsic fingerprint detection technique. This paper concludes that

these techniques are even useful to detect small patches, although failed to detect re-sampling when the image is JPEG compressed.

S.Murali ,Govindraj B. Chittapur, Prabhakara H. S and Basavaraj S. Anami[8] proposed two methodologies to identify the forged regions in images even when only the forged image is given. One is based on JPEG compression analysis in which block-based DCT is used and results are easily noticeable. Second method is based on direction filter which uses edge detection and horizontal & vertical projections are calculated, combining them feature map is extracted from which forgery region is displayed. This method is expanded to other formats like png, bmp, etc.

Jessica Fridrich, David Soukal, and Jan Lukas [9] described a method which helps to detect the forged image even if the image is saved in JPEG format after applying retouching operations. They proposed two algorithms, one that uses exact match for detection and other is based on approximate match. Under approximate block matching, exhaustive search and autocorrelation are explained. In exhaustive search, the image and its circular shifted version are overlaid finding closely matching segments. And in autocorrelation, original & copied segments will generate peaks for the shifts that correspond to copied segments. Both methods are simple but abandoned in favor of exact block matching algorithm. Second algorithm is based on exact match that identifies those segments which match exactly, it also forms basis for robust match as well.

Li Kang and Xiao-ping Cheng [10] presented a blind detection method which uses block matching procedure to divide the image into equal sized blocks. Then by using real matrix, single value feature vector is obtained and sorted lexicographically. For making singular value decomposition better only significant values are selected and rest are discarded. Later, a similarity matching is done based on similarity coefficient measure, threshold value is chosen depending on correlation coefficient. If the correlation coefficient value is less than threshold value, then no copied region is there otherwise detection result shows the copied blocks. Thismethod ensures greater detection capability and anti-noise capability.

TABLE.I Gives description of several copy move image forgery detection techniques.

Ref. No.	***Purpose***	***Techniqueused***	***Merits***	***Demerits***
1.	CMF detection which can sustain preprocessing attacks	DyWT and SIFT	Can detectmore number of keypoints for efficient matching.	False positive rate is more.
2.	To detect additional noise and JPEG quality changed images	DWT and filtering	Robustness	Takes into account only shifting of copied regions.
3.	To detect double quantization effect hidden among DCT coefficients	DCT	Fast computation (block size should be smaller)	Large block size, more execution time. & only applicable to gray scale images.

4.	Highly textured images with different types of transformations and shapes of copied regions	Multi-resolution WLD and SVM for classification purpose	Gives better discrimination than single resolution , better edge detection, robust to noise change and illumination	Computationally complex, and even impossible for images of bigger size
5.	To detect CMF in high resolution images	SURF and KD-tree for multidimensional data matching	Results in minimum false rate	More feature vectors so more probability of matching wrong block is more
6.	To select region of interest(ROI) automatically	Segmentation, EM algorithm to find probability map	Gives better results after skewing transformations, and re-sampling, etc.	Small regions detection is difficult
7.	Basic image manipulations	FFT and intrinsic fingerprint detection technique	Computation speed fast, can detect small patches	JPEG compressed image tampering is difficult
8.	JPEG compression analysis	DCT and edge detection using direction filter	Valid for various formats	Slow
9.	To detect if images are compressed in lossy format	Exhaustive search, Autocorrelation	Accuracy and robustness	Applicable to small images only
10.	Automatic detection of copied regions	Singular value decomposition and correlation	Strong detection, anti-noise capability	Threshold value selection is difficult

IV. CONCLUSION:

There is a growing need for passive image authentication techniques, and many modern algorithms have been proposed to solve the issue of image authenticity. This paper surveyed the algorithms that were dedicated to copy-move forgery because it is the most common forgery type. For comparison purposes, one algorithm in each category was considered to represent its category. The algorithm with the best performance and features within its category was selected.Table 1 presents a comparison between these algorithms according to the general pipeline stages. From the survey it is concluded that DCT is computationally fast and it gives good results for gray scale images.

REFERENCES

[1] Mohammad FarukhHashmia, Vijay Anand, Avinas G. Keskar "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform" 2014 AASRI Conference on Circuit and Signal Processing (CSP 2014)

[2] Ms. P. G.Gomase, Ms. N. R.Wankhade"Advanced digital image forgery detection:a Review" International Conference on Advances in Engineering & Technology, (ICAET-2014)

[3] Ashima Gupta, NisheethSaxena, S.K Vasistha"Detecting Copy move Forgery using DCT" International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013

[4] Muhammad Hussain, GhulamMuhammada, Sahar Q. Saleh, Anwar M. Mirza, and George Bebis"copy-move image forgery detection using multi-resolution weber descriptos" Eighth International Conference on Signal Image Technology and Internet Based Systems 2012

[5] B.L.Shivakumar and Lt. S.SanthoshBaboo"Detection of Region Duplication Forgery in Digital Images Using SURF" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011

[6] P. Subathra, A. Baskarand D. Senthil Kumar"detecting digital image forgeries using re-sampling by automatic region of interest (ROI)" ICTACT journal on image and video processing, May 2012, volume: 02, issue: 04

[7]S.DeviMahalakshmi, K.Vijayalakshmi, S.Priyadarshini" Digital image forgery detection and estimation by exploring basic image manipulations" Digital Investigation 8(2012)

[8] S.Murali , Govindraj B. Chittapur, Prabhakara H. S and Basavaraj S. Anami"comparison and analysis of photo image forgery detection techniques" (IJCSA) Vo2, No.6, December 2012

[9] Jessica Fridrich, David Soukal, and Jan Lukáš "Detection of Copy-Move Forgery in Digital Images"Air Force Research Laboratory, Air Force Material Command, USAF, under a research grant number F30602-02-2-0093

[10] Li Kang and Xiao-ping Cheng " Copy-move Forgery Detection in Digital Image" 3rd International Congress on Image and Signal Processing, IEEE-2010.