M-SIFT:A Detection Algorithm for Copy Move Image Forgery

Tarman
Department of electronics and communication engineering
Chandigarh Engineering College
Mohali
tarmangarg@gmail.com

Hardeep Saini
Department of electronics and communication engineering
Chandigarh Engineering College
Mohali
hardeep.ece@cgc.edu.in

Abstract— **Forgery is not a new concept but from the very start it has been there whether it is in documents, images, art, or literary etc. Threats against digital images has increased to that extent that they require serious attention. Copy move forgery being the most dangerous one, is affecting world of digital images as this is hardest to detect. We first discuss and demonstrate image forgery types, discuss detection methods and their shortcomings, and then discuss the idea of using Keypoint based method M-SIFT which is an improved version of SIFT. Additionally, we provide implementation and performance analysis of suggested algorithm.**

Keywords—Image Forgery Detection; Copy-Move Forgery; DCT; QCD; SVD; M-SIFT

I. INTRODUCTION

Images play a vital role for conveying trustworthy information but due to fast growing image processing field new image editing softwares are available such as Photoshop, photo editor, GIMP etc [13]. Due to these softwares image forgery has become effortless. Image forgery means manipulating the image content according to one's own desire. There is a huge network of digital images all over the internet but we just can't believe what we see in these images, we need proof of their authenticity. Every invention has its own pros or cons and so is with Image editing tools. Christophe Gilbert, Erik Alms, Riccardo Bagnoli are such artists who use image editing tools to create very impressive advertisements and images that convey deep knowledge. But there are also people who manipulate images to harm someone's life and destroy their reputation. Actors, Leaders or famous personalities are more victims of these forgeries than normal people. Crime investigations also cannot use images as prime evidences because they could be forged. Image forensics deals with such situation as they can check the authenticity of images. Image forensics is a research area trying to resolve the imposed problem of authenticity assuming that different imaging devices or processing would introduce uniform inherent patterns which are consistent in original clean images and would become unstable after manipulations. These instabilities can be used as evidence for forgery detection [5].

II. TYPES OF IMAGE FORGERIES AND DETECTION METHODS

There are many types of forgeries such as Image retouching, Image splicing, Copy-move, Enhanced, Morphing etc [1]. Image retouching is the most harmless type of forgery because content is not touched only features are enhanced to make an object or thing or person look more attractive. Copy move forgery is the most difficult to detect as a particular part of an image is copied and pasted somewhere else in the same image. A CMFD is easy to create. Additionally, Both the source and the target regions originate same from the same image, so properties like color temperature, noise, illumination effects are expected to be well matched between the manipulated and source image[3]. Image editing tools provides a large number of features for example scaling, resizing, rotation, affine transformations, color contrast etc. Editing images seem so real that it can fool anyone. Digital watermarking and digital signature are active methods which can be used to ensure integrity of the image. Digital watermarkers use a checksum schema in that it can add data into last most significant bit of pixels or can add a maximal length linear shift register to pixel data [4].Digital signature is generated by a producer-specific private key such that it cannot be manipulated [7].But these are only efficient for images captured by some specially equipped cameras. So there was a need of more dynamic methods that can detect forgery in all types of image whether image is compressed or scaled. Passive methods overcome all the shortcomings of active methods. Because it require no previous information about the image [12].

III. SHORTCOMINGS OF EXISTING METHODS

Detection methods are broadly classified as Keypoint and blockbased method. DCT,DWT, FMT, PCA, SVD are block

978-1-5090-5838-9 /17 $31.00 © 2017 IEEE

based methods.DCT(Discrete cosine transform) are only good for detecting forgeries in small texture areas.FMT(Fourier millen transform) could not detect forgery if the forged part is rotated and scaled greater than 10 degree.PHT(Polar harmonic transform) cannot detect forgeries if they are not rotated at an angle of 90 degree.QCD(Quantization coefficient decomposition) cannot detect rotated or scaled part before copy pasting it somewhere else in the image.Curvelet based method cannot detect forgeries if image is compressed.[14].DWT(Discrete wavelet transform) is useful in applications where data is compressed but not efficient for filtering, detection, pattern, recognition, texture analysis[6].PCA(Principal component analysis) does not detect forgeries if images are jpeg compressed but DCT performs very well here[2]. Keypoint based methods include SIFT, SURF, U-SURF etc. SIFT (Scale invariant feature transform) is very efficient technique but slow in processing. SURF (Speeded up robust feature) seems to be very fast method but not very robust[11].Combination of keypoint and blockbased techniques also proves to be efficient in some cases such as DWT have been used with Scale Invariant Feature Transform for copy move forgery detection[8]. SIFT (Scale Invariant Feature Transform) descriptor is used to extract key-point features from input image, but it needs more processing time to extract or detect copied region.ORB (oriented FAST and rotated BRIEF) is fast as compared to SIFT descriptor[16].Comparative analysis of various detection techniques has also been discussed in [13].

IV. SCALE INVARIANT FEATURE TRANSFORM AND ITS LIMITATIONS

SIFT method has been derived from the scale-space theory, is a local feature extraction algorithm. Looking at the extreme point, extract the location, scale and rotation invariant in the scale space [15]. Existing SIFT is a highly robust method which can detect any geometrical transformations but to a limit.

SIFT Algorithms works in following steps:

1. Image conversion and pre-processing

Any colored image is given as input. First, it will be converted into grayscale format. Then some preprocessing will be done by resizing it and adding Gaussian blur to it.

2. Features extraction, orientation assignment and feature matching

Scale space extrema detection method is used. Blur the input image and keeps shrinking it. Adding blur helps in extracting more keypoints.4 or 5 octaves are enough for one image.

$$L(x,y,\sigma)=G(x,y,\sigma)*I(x,y)$$

L represents the new formed image after adding blur into I image [9].DOG(Difference of Gaussians) are calculated by calculating second order derivatives of blurred images. This will locate edges and corners on image. Locate maxima and minima of blurred images. Take Taylor expansion of DOG images. Keypoints with high intensity values is chosen and all the low contrast values are rejected which usually lie on edges. To provide rotation invariance, Orientations are assigned to them which act as finger print for each keypoint. For sample image L(x, y, σ) at scale σ, Gradient magnitude and gradient orientation calculated as per given formulas respectively.

$$m(x,y)=[(L(x+1,y)-L(x-1,y))^2+ L(x,y+1)-L(x,y-1))^2]^{1/2}$$

$$\Theta(x,y)=\tan^{-1}(L(x,y+1)-L(x,y-1)/L(x+1,y)-L(x-1,y))$$

After calculating gradient magnitude and assigning orientation (o), final SIFT (f) descriptors will be calculated. Every feature descriptor will have a histogram f of 128 elements, obtained from a 16 x 16 pixel area around the corresponding keypoint. Total n keypoints will be generated having information about scale(σ),canonical orientation(θ) and descriptor(f).

Feature matching of a keypoint is done by identifying its nearest neighbor from all the other (n −1) key points of the image, which is the key point with the minimum Euclidean distance in the SIFT space [10].

3. Clustering

To detecting possible copied areas, an agglomerative hierarchical clustering is performed on spatial locations (i.e. x, y coordinates) of the matched points. Hierarchical clustering creates a hierarchy of clusters which may be represented by a tree structure. The algorithm starts by assigning each key point to a cluster; then it computes all the reciprocal spatial distances among clusters, finds the closest pair of clusters, and finally merges them into a single cluster. Such computation is iteratively repeated until a final merging situation is achieved. The way this final merging can be accomplished is basically conditioned both by the linkage method adopted and by the threshold used to stop cluster grouping [10].

4. Geometric transformation

After identifying forged region, type of geometric transformation is detected whether it is scaling or rotation or illumination changes using RANSAC (Random sample consensus) algorithm.

Above discussed technique SIFT can detect if a particular image is forged or not and can also detect type of attacks done to it. But as it is known that SIFT alone needs high computational time to extract or detect copied region [11, 16].Also SIFT method can detect rotational attack only upto 40 degree. Greater than 40 degree attacks are hard to find.

978-1-5090-5838-9 /17 $31.00 © 2017 IEEE

So there is a need to develop such system that can detect forgery greater than 40 degree. Proposed technique works by choosing best threshold values and improvement in clustering algorithms.

V. DESIGN AND IMPLEMENTATION OF PROPOSED METHOD - MODIFIED SIFT (M-SIFT)

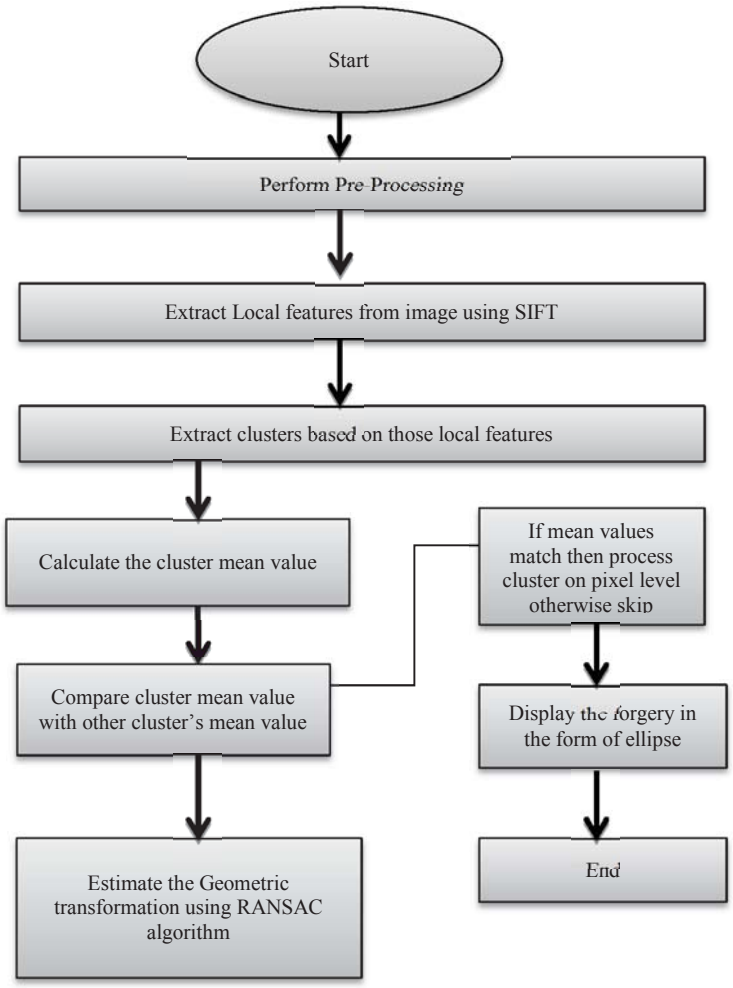


Fig. 1. Flow chart of proposed methodology

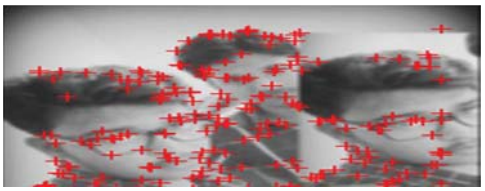
M-SIFT have following steps:

- Input an image
- Extract features using SIFT
- Keypoint matching is done using Euclidean distance approach
- Clustering is done for detecting cloned areas
- Cluster mean values are calculated and compare with each other
- If cluster mean value match then process on pixel level otherwise skip
- Geometric transformation is estimated using RANSCAC algorithm

(Original image, mobile captured image)Image from dataset 'forgery'

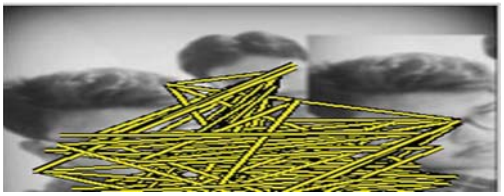
(Copy move forged image made by coping one part of image somewhere else in the same image)

(a) Input image and preprocessing



(b) Extract local features from all over image

(c) Extract clusters based on local features, calculate the clusters and cluster mean values



(d) Estimate Geometric transformation using RANSAC

(e) Display the forgery in the form of ellipse

Fig.2.Overview of M-SIFT, matched pairs and clusters

978-1-5090-5838-9 /17 $31.00 © 2017 IEEE

VI. PERFORMANCE ANALYSIS OF M-SIFT USING VARIOUS PARAMETERS

We have created a dataset named 'forgery' consists of different images some of which are forged and some are original. These images have been taken from various standard and non standard datasets. Results on this dataset have been collected after a lot of calculations. Various attacks of forgery have been applied to this dataset check the performance of the proposed system.

Table1. Different combinations of Geometric transformations applied on images of the proposed dataset.

Attack	Rotation	Scale(x)	Scale(y)
A	0	10	10
B	0	50	50
C	20	1	1
D	90	1	1
E	180	1	1
F	20	2	2
G	90	10	10
H	0	1	1

The above table represents the various combinations of attacks comprising of Rotation and Scaling along with image forgery. Rotation attack in the table is specified in the degrees while scaling attack is specified in form of percentage. We have applied the attacks according the values given in the above table to detect the forgery in the given input image. We have defined the various attacks combinations with Alphabets from A to H.

Table 2. No. of images representing the attacks and accuracy detected by the system on different images

Attack	No. of forged images	Forgery detected	Accuracy
A	15	15	100
B	15	15	100
C	10	10	100
D	6	5	83
E	5	4	80
F	20	20	100
G	10	9	90
H	25	24	96

Above table specifies the total number of forged images, number of images in which forgery is detected and their corresponding accuracy according to the given attack format. Various attacks from table 1.1 have been applied on various images as given in above table. Above table represents the overall results in form of accuracy of the proposed system.

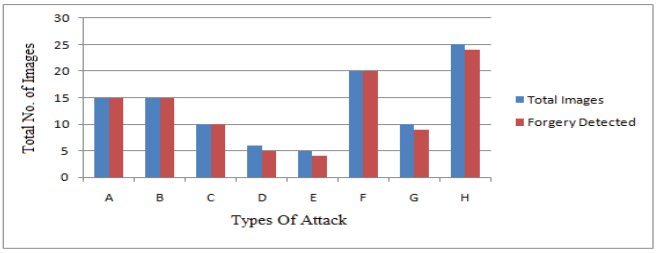


Fig.3. Graph representing the accuracy of the proposed system on different attacks

Accuracy = (No. of Forged Images/No. of forgery Detected Images)*100

Precision = (No. of Forged Images/No. of total forgery detected images)*100

Recall = (No. of Forged Images/No. of correct forgery detected images)*100

Table 3. Proposed System performance evaluation on forgery below 40 degree angle

Image Name	Accuracy	Recall	Precision
Tampered 1	100%	100%	100%
Tampered 2	100%	100%	100%
Tampered 3	100%	100%	100%

Table 4. Proposed System performance evaluation on forgery above 40 degree angle

Image Name	Accuracy	Recall	Precision
Tampered 1	95%	100%	99%
Tampered 2	93%	100%	98%
Tampered 3	94%	100%	98%

Table 5. Table of comparison between existing and proposed system

Parameter	Existing System	Proposed system
Max. angle detected	40 Degree	180 Degree
Scaling	1.4	1.5
Scaling+ Rotation	1.4+20	1.5+90
Precision	96.85	98
Recall	100%	100%
Accuracy (below 40 degree)	100	100
Accuracy (above 40 degree)	Forgery not detected	93.62%

VII. Conlcusion and Future scope

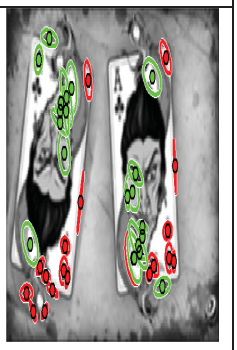
Original Image	Image with attack	Forgery detected
 (a) retail		
 (b)copy move image forgery detection matlab code		
 (c)playing cards ace wallpaper hd		

Fig. 4. Snapshot of detection of tampered digital images from dataset 'forgery'

(a) Tampered 1-Copy pasted
(b) Tampered 2-Copy pasted and tilted to one direction
(c) Tampered 3-Copy pasted rotated at more than 180 degree

A. Conclusion

In the proposed work, we have implemented the Modified SIFT (M-SIFT) algorithm to detect the copy move forgery in the digital images. Proposed system is tested on various images of standard dataset. Overall Accuracy of the proposed system is calculated to as 92% which is better than that of existing algorithms. It is concluded that the proposed system shows considerably high improvement than the previous systems. Average time taken to process the input by the proposed system calculated as 45 seconds which is again less than that of existing systems. Proposed system can detect forgery if copied part is rotated at 180 degree while existing systems detect upto 40 degree. In proposed work, we use clusters and their mean values to find the forged area within the image to reduce the overall processing time. Proposed system also shows good accuracy in the images that can contain scaled forgery or forgery with geometric transformations.

B. Future Scope

In future, system can be enhanced to minimize the processing time to detect the forgery in the images to few seconds or even microseconds. E-SIFT and SURF algorithms can be combined to improve the overall performance of the proposed system. In future, the proposed system can also be improved in such a way that it can detect forgery with the attack value of more than 98 degree. Proposed system takes too much time if the image resolution is very large and it cannot detect the forgery in the images if three attacks are performed simultaneously, in future proposed system working can be enhanced to deal with above issues and make system work more efficiently.

978-1-5090-5838-9 /17 $31.00 © 2017 IEEE

REFERENCES

[1] Salam A.Thajeel, Ghazali Bin Sulong , "STATE OF THE ART OF COPY-MOVE FORGERY DETECTION TECHNIQUES: A REVIEW" ,IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, 2, November 2013 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784

[2] Ashima Gupta, Nisheeth Saxena, S.K.Vasistha, "Detecting Copy move forgery using DCT", International Journal Of Scientific and Research Public ations (IJSRP),ISSN: 2250-3153,Vol. 3,Issue 5,May-2013.

[3] Vincent Christlein,Christian Riess,Johannes Jordan, Corinna Riess,Elli Angelopoulou, "An Evaluation of Popular Copy-Move ForgeryDetection Approaches" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 26 NOV 2012 , pp-126.

[4] Nikhilkumar P. Joglekar, Dr. P. N. Chatur , "A Compressive Survey on Active and Passive Methods for Image Forgery Detection", Internation journal pf engineering and computer science,ISSN:2319-7242,vol 4,issue 1,jan. 2015,pp-10187-10190.

[5] Archana V. Mir, Dr S. B. Dhok, Dr N. J. Mistry and Dr P. D. Porey, "Catalogue of Digital Image Forgery Detection Techniques, an Overview",ELSEVIER 2013,Proc of int.conf. on advances in information technology and mobile communication,pp-502-508.

[6] Najah Mohammad et al, "COPY MOVE FORGERY DETECTION USING DYADIC WAVELET TRANSFORM" Eighth International Conference Computer Graphics,Imaging and Visualization,DOI 10.1109/CGIV.2011.29,103-108,2011

[7] Harpreet kaur and Kamaljit kaur, "A Brief Survey Of Different Techniques for Detecting Copy Move Forgery", International Journal Of Advanced Research in Computer Science and Software Engineering, (IJARCSSE),ISSN:2277 128X ,Vol. 5,Issue 4,2015,Page no. 875-882.

[8] Lakhwinder Kaur Bhullar, Sumit Budhiraja and Anaahat Dhindsa, "DWT and SIFT based passive copy move forgery detection", International Journal Of Computer Applications (IJCA), Vol. 95,No.23, June-2014.

[9] Rajeev Rajkumar and Kh Manglem Singh " Digital Image Forgery Detection using SIFT feature",IEEE(2015)), DOI **:** 10.1109/ISACC.2015.7377340, 11 January 2016

[10] Irene Amerini, Lamberto Ballan, Student Member, IEEE, Roberto Caldelli, Member, IEEE, Alberto Del Bimbo, Member, IEEE, and Giuseppe Serra, "A SIFT-based forensic method for copy-move attak Detection and transformation recovery" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 6, no.1, Sep. 2011, pp 1-12

[11] Ramesh chand pandey et al, "Fast and robust passive copy move Forgery Detection using SIFT feature",IEEE(2015), DOI **:** 10.1109/ISACC.2015.7377340, 11 January 2016

[12] Rakshita Singh and Mehul Thakkar,"Copy move Image Forgery Detection Techniques:Survey", International Journal Of Modern trends in Engineering and Reseach), e-ISSN:2349-9745,Vol. 3,Issue 4,Apr. 2016),pp 654-657.

[13] Tarman & Hardeep saini,"A Review on Various Techniques of Image Forgery Detection",2nd International conference on research trends in engineering,applied science and management(ICRTESM-2017),23April,2017,ISSN-2394-3386,volume 4,issue 4,pp-490-493

[14] Anuja Dixit and R.K.Gupta, "Copy-Move Forgery Detection using Frequency-based Techniques:A Review" International Journal of Processing, Image Processing and Pattern recognition(IJSIP) , ISSN-2005-4254,Vol.9,No.3,2016,pp.71-88.

[15] Xue Leng* and Jinhua Yang, "Research on improved SIFT algorithm" Journal of Chemical and Pharmaceutical Research, 2014, 6(7):2589-2595, ISSN : 0975-7384.

[16] Rajdeep Kaur amd Amandeep Kaur, "Copy-Move Forgery Detection Using ORB and SIFT Detector" International Journal of Engineering Development and Research, 2016 IJEDR | Volume 4, Issue 4 | ISSN: 2321-9939,pp-804-813.