Adaptive Keypoint Selection for Detection of Tampering in Images and Videos

Sonal Patil, K. N. Jariwala

Abstract: ***Tampering with images and videos for duplicating content and copyright infringement has become a very common problem for original content producers. The main issue with duplication and forgery is that, due to the advancement of forging techniques, it is being increasingly difficult in terms of both computational power and algorithmic complexity to detect and trace the forgeries with good level of accuracy. In this paper, we propose an adaptive keypoint based approach to detect the presence of forgery in images. Our approach is independent of the input dataset, and provides good level of accuracy for forgery detection. The system is tested on REWIND dataset, and an accuracy of more than 85% was observed. Our approach can be further extended to incorporate machine learning in order to improve the accuracy.***

Index Terms*: *Tampering, forgery, keypoint, REWIND, complexity.

I. INTRODUCTION

These days, advanced pictures are the chief wellspring of data and they are the quickest methods for data pass on as "words generally can't do a picture justice". Picture has procured the notoriety for being unarguable proof. Albeit quick development in the field of picture altering programming, for example, Adobe Photoshop, Picasa, and so on which permits even generally unpracticed clients to process advanced pictures in an exceptionally advantageous manner which can test the validness of an image.Tampered pictures are utilized not exclusively to make extraordinary photographs for entertainment only, yet in addition in different backgrounds like giving security to substantial records and can be utilized for misdirecting individuals as altering in the picture changes the visual message of the picture.

Anyway the credibility confirmation of picture is especially required in different applications for an occasion, the reliability of picture has an indispensable job in courts, where they assume job of proof. Consistently papers and magazines rely upon computerized pictures.

In the therapeutic field, doctors settle on basic choices dependent on computerized pictures and it can likewise be a piece of helpful records, or as cash related reports. So there is a pressing need to recognize the legitimacy and uprightness of advanced pictures. In this sense, picture forgery recognition is one of the basic destinations of picture crime scene investigation.

In the field of drug: Reports of patients are exceptionally private and are constantly expected to be bona fide. Therapeutic pictures are created in the majority of the cases as confirmation for wretchedness and guarantee of illness and doctors settle on basic choices dependent on advanced pictures.

- In the field of instruction: Students completed extensive measure of forgery with their records for their own advantage. This exasperates the security of the administration which can be unraveled by recognizing the altering in the picture.

- In the field of horticulture: Tampering is additionally finished with the distinctive pictures utilized amid the preparation of the ranchers which results to the misguidance to the rural understudies.

- In the lawful cases: The criminal equity, for which photos are regularly introduced as court proof. For this, realness check of each and every bit of proof should be strong. Altering a picture which is going about as proof can prompt settle on off base choice.

- In the field of fund: The back business can profit by such picture forgery identification application as they need to process and dissect various exchange archives each day.

In this way, such zone requires picture forgery location apparatus that are both quick and solid to deal with such situation.

SORTS OF DIGITAL IMAGE FORGERIES

The control or altering in the advanced picture is named as picture forgery. Advanced picture forgery can be arranged in Image Retouching, Image Splicing (Compositing), Image Cloning (Copy-Move).

- Image Retouching: In this sort of forgery picture is improved by performing

Revised Manuscript Received on May 23, 2019.

Sonal Patil, B.E., M.Tech in CSE, Pursuing PhD in Computer Engineering from S.V.N.I.T., Surat.

Dr. Krupa N. Jariwala, B. Tech., M.Tech and PhD in Computer Engineering. Assistant Professor in Computer Engineering Department, S.V.N.I.T., Surat.

slight changes in the picture or decreasing certain highlights in the image. Light changes should not affect the recognition process of forgery detection

Fig(1): Example of Image Retouching (a) original image (b) tampered image

Image Splicing (Compositing): In this kind of forgery sections of two unique pictures are consolidated to create a solitary fashioned image. Image joining strategy may change the visual message of advanced pictures more forcefully than picture modifying.

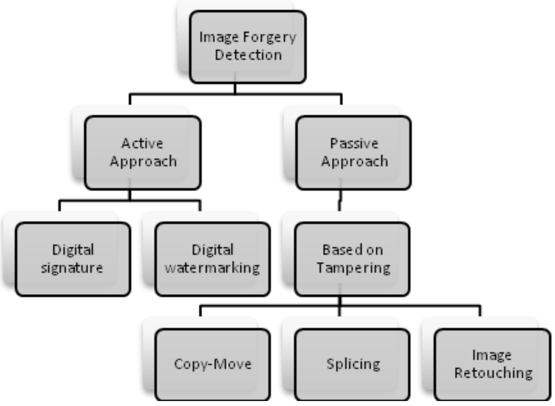
Fig(2): Example of Splicing forgery (a)Original Image (b) Original Image and (c)Tampered Image.

Image Cloning (Copy-Move): n this kind of forgery, picture is controlled by replicating a piece of picture and gluing it into another piece of the equivalent image. The reason for such altering is to copy or hide a specific article in that picture

Fig(3): Example of Copy-Move forgery (a) original image (b) tampered image

TYPES OF IMAGE FORGERY DETECTION TECHNIQUES

Advanced picture forgery location systems are characterized into dynamic and latent methodologies. In dynamic methodology, the advanced picture requires some pre-handling, for example, watermark installing or open mark age at the season of picture procurement or before dispersed to people in general which would confine dynamic methodology by and by. Additionally, numerous cameras are not refined with these highlights which results disappointment of dynamic methodology. Then again detached techniques work without pre-inserted data like computerized watermark or advanced mark.



Fig(4) : Categories of Image Forgery Detection Techniques

II. LITERATURE REVIEW

In [1] the square discrete cosine change is should have been connected on the picture. In the wake of applying the DCT the areas that have been copied are identified. DCT coefficients are then orchestrated and arranged lexicographically and assembled by likeness of squares having the equivalent spatial counterbalanced in the picture thusly the copied areas are recognized. In [2] which is a comparable methodology foremost part investigation (PCA) is done on little picture squares having settled size. This procedure is utilized to lessen the measurements for the portrayal. Some computationally effective calculations have been produced.

In [3] researchers depicts that when picture control is done appropriate scenes, pivot, scaling is done on picture which includes new connections between's the pixels in the area which are explicit and requested intermittently, as this these relationships are not a typical wonder, the event of such relationships and nearness of such explicit arranged relationships can fill in as a proof to distinguish the picture has been doctored. Introduction connected in order to smooth the picture and to make the picture look a persuading and engaging in order to evade visual framework. Be that as it may, the utilization of these interjection calculations prompts straight conditions among the gatherings of neighborhood areas. This degree of these conditions changes because of the length of the occasional cycles, which is a reliant capacity of the looking like rate. The resampling location includes utilizing direct indicators that utilization intermittent antiquities to recognize resampling. Popescu and Farid locator utilizes a straight indicator which appraises each example's esteem roughly as the weighted whole of its encompassing examples.

In [4] researchers distinguish these prompted associated higher request relationships as a methods for identifying the nearness of a non-linearity. Usually a squaring function is used to find similarity values for the blocks. On the off chance that such higher request relationships are feeble in "common" flags, their quality can be utilized as a sign of altering. [7] and [32].

In [5] researcher misuses the way that pictures have doubtful areas that have distinctive gadget marks from different locales if the picture has been grafted . For identifying the joined locales the technique that can be utilized are picture division and vigorous recuperation of camera marks from each area. Any mainstream division apparatus can be utilized for picture division, Normalized Cuts [6], however different strategies, for example, Mean Shift [7] might be considered. For getting the gadget mark and estimating consistency, researchers in [5] utilize the single channel CRF estimation and a cross fitting plan. The picture to be tried is portioned into various areas utilizing Normalized Cuts [6], at that point CRF estimation is done in each locale. For checking if a limit section in the middle of any two neighboring districts is unique or joined. The cross fitting is connected in the middle of CRF from one district and the information tests of another area and utilizing these to depict a limit fragment. SVM is utilized to take these component vectors and utilizing them to arrange whether the limit fragment is unique or joined. The order aftereffects of the every one of the sections are then on the whole used to finish up if the picture is joined or unique, and follow the Skeptical locales which are named grafted ones.

At the point when a picture is caught utilizing an advanced camera, the data that is caught with respect to the scene experiences the distinctive camera parts. Every segment is a piece of the data handling framework refreshes the info utilizing a calculation utilizing a which is specific and by utilizing explicit parameter set and which forgets some characteristic fingerprints[8]. While making an altered picture a succession of post camera handling activities like separating, resampling, pressure and so on which can be connected to the whole picture or to particular districts of the picture locally. These tasks leave unmistakable indication in the picture at last got and which can be identified by making utilization of classifier dependent on edge and by contrasting the control assessed and the reference pattern[9].

Most usually and broadly utilized Color channel exhibit is the Bayer exhibit [11], which utilizes three shading channels: red, green, and blue..As a solitary shading test is being recorded, the staying two shading tests are assessed from the neighboring examples. A straightforward direct model for the intermittent connections by CFA insertion can be considered. Each added pixel is connected to the weighted total of pixels neighboring the pixel which is being considered. This model simple for choosing parameters just as can estimated the CFA insertion calculations to a decent degree. The particular type of the relationships is realized then it is anything but difficult to figure out which tests are connected with their neighboring examples.

Likewise, in the event that it is realized that examples are corresponded with their neighboring examples, the specific sort of the connections can be resolved. The two cases don't exist as a rule. The desire/augmentation calculation can be utilized for evaluating both at the same time. The occasional example of pixels is exceedingly related with pixels of their neighborhood in the first picture. On the off chance that they are not profoundly connected it tends to be considered as a proof of tampering.[10].

As depicted in [12] and [13] , the distinction in the proportion of pressure and quality can be utilized to perceive the source camera. The channels are divided into 8x8 window. These qualities are changed over from unsigned to marked whole numbers. By utilizing a 2-D discrete cosine change (DCT) each square is then changed over to recurrence space. This is proved in [14], that such a recurrent method is indeed useful for image forgery analysis.

For any computerized picture control it is an absolute necessity perquisite that a picture ought to be stacked into a photograph altering programming program and again should be resaved. Since JPEG encoding plan is ordinarily utilized, a large portion of the pictures are put away in the JPEG organize, there exists a high likelihood that both the genuine pictures and controlled pictures are put away in JPEG arrange. If so, the picture that has been doctored is compacted twice. This nature of the lossy pressure plan of the JPEG picture arrange, actuates explicit relics in the doubly compacted picture which are missing in independently packed pictures. This curios prompted can fill in as a proof of some control [15][16]. In [17] , the researchers portray the particular nature or highlights of the blocking antiques by utilizing pixel esteem contrasts inside and past square outskirts. The distinctions is lesser inside the squares and more noteworthy crosswise over squares. When editing and recompression is connected, another kind of blocking curios is presented that may don't really line up with the true picture's limits. In [18] , the researchers underline and diagram the discovery of limited controls from changeability in blocking antiques . In the event that picture is viewed as unique one, the dimension of quantization is first evaluated for every one of 64 DCT frequencies. The irregularities between DCT coefficients and assessed dimension of quantization over the picture are utilized to identify doctored areas.

The essential point is close to the focal point of the picture for the first pictures. The foremost focuses moves relatively when picture or articles in the scene are controlled. This distinctions in the assessed central point can be utilized as proof of altering. In [19] , the researchers depict a path for estimation of a camera's primary point by utilization of picture gotten by a couple of eyes (i.e., two circles) or other planar geometric shapes.

III. PROPOSED ALGORITHM

The proposed adaptive key-point based algorithm is designed using the following steps,

Key point extraction

Training the system

Evaluation of forgery using adaptive key point selection

Initially the input images are given to a key point extraction algorithm, which evaluates Maximal Stable Extremal Regions (also knows as MSER), and applies Speed up Robust Features (SuRF) method on each of these regions. The SuRF method evaluates keypoints for each of the regions, the distribution and values of these key points assists in evaluation of the image properties.

Once the keypoints are evaluated, they are tagged using the training phase. The training phase basically stores information about the image keypoints along with the tag whether the image is forged or not, and if it is forged then the type of forgery (splicing, copy-move, etc.) with which the image is tampered. This information helps in identification of the keypoints which are later used for comparison by the adaptive keypoint selection algorithm and identify the forgery type.

The tagged database along with the full keypoint features of the image to be tested are given to the adaptive keypoint classifier. The adaptive keypoint classifier works via the following process,

The query image features are distinguished with the help of the feature length for a given region

For each region, the number of keypoints which are equal to the keypoints in the database are compared using standard keypoint matching and a score value S1 is calculated based on the number of features matched

For other unequal length features, the following process is followed,

If the number of features of the query image are less than the number of features of the database entries, then the database entries are trimmed and comparison is done to find out the score S2

If the number of features of the query image are more than the number of features of the database entries, then the input image feature entries are trimmed and comparison is done to find out the score S2

The total score of the image is evaluated using, S=S1+S2+S3

This is done for each database entry and scores are evaluated for all of them

Finally the entry with maximum score is selected and classification is done. Based on this classification, we obtain whether the input image is forged or non forged

Results of this technique are evaluated on various datasets and then compared with standard datasets in the next section.

IV RESULTS AND OBSERVATIONS

We tested the proposed algorithm on CASIA Tamper Detection Dataset V2, and used 70/30 ratio of training to testing images. The algorithms under comparison are DCT, Mean Shift and PCA. The following table shows the result of accuracy for the system,

Images tested	Accuracy (%) DCT	Accuracy (%) Mean Shift	Accuracy (%) PCA	Accuracy (%) Proposed
10	80	80	70	80
25	84	84	76	86
40	85	86	78	86
50	82	83	78	86
75	84	85	79	88
100	82	80	80	94
200	79	82	83	94
500	79	83	84	95

Table 1. Accuracy comparison

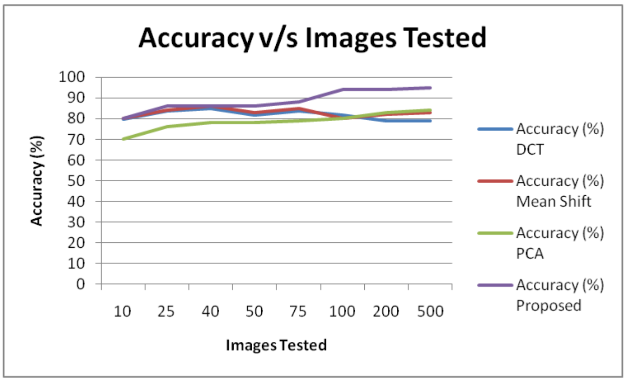


Figure 4. Comparison of accuracy v/s images tested

From the above table we can observe that the proposed algorithm outperforms others by a descent margin. The results hold true for low to high number of images, and can be extended to any other datasets. The proposed algorithm was also compared in terms of delay with the same set of standard techniques, and the following results were obtained,

Images tested	Delay (ms) DCT	Delay (ms) Mean Shift	Delay (ms) PCA	Delay (ms) Proposed
10	1.20	1.50	1.35	1.01
25	1.50	1.80	1.65	1.24
40	1.80	2.30	2.05	1.54
50	1.90	2.80	2.35	1.76
75	2.30	3.90	3.44	2.41
100	3.50	4.50	4.44	3.11
200	6.70	8.40	8.39	5.87
500	12.60	15.20	15.44	10.81

Table 2. Delay comparison

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

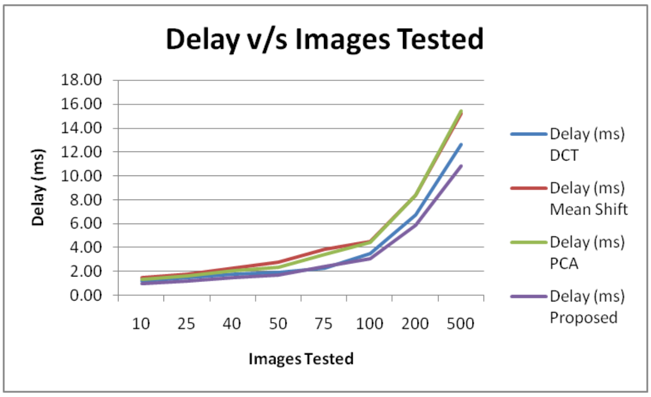


Figure 5. Delay v/s images tested

The proposed algorithm has lower delay when compared to other standard techniques, due to the fact that the classification is done with less number of features as compared to DCT or other techniques. As the number of features are less, thus the delay for comparison is usually less. Thus our technique can be used for real time evaluation of forgery, even in videos or high speed imagery.

V. CONCLUSION

From the results, it is clear that the proposed algorithm outperforms the other standard algorithms by a good margin in terms of both accuracy and delay of comparison. Thus the proposed algorithm can be used for further evaluation of other forgery types, and can be extended for the case of video forgeries or other high speed image forgery applications. The classifier can also be changed in order to further improve the accuracy and reduce the number of computations required for comparison with the dataset.

REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukás, “Detection of copy move forgery in digital images,” in Proc. Digital Forensic Research Workshop, Aug. 2003.

[2] A.C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.

[3] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting traces of re-sampling,” IEEE Trans. Signal Processing, vol. 53, no. 2, pp. 758–767, 2005.

[4] H. Farid, “Detecting digital forgeries using bispectral analysis,” AI Lab, Massachusetts Institute of Technology, Tech. Rep. AIM-1657, 1999.

[5] Y.-F. Hsu and S.-F. Chang, “Image splicing detection using camera response function consistency and automatic segmentation,” in Proc. Int. Conf. Multimedia and Expo, Beijing, China, 2007.

[6] Jianbo Shi and Jitendra Malik, “Normalized cuts and image segmentation,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 8, pp. 888–905, 2000.

[7] C. Yang, R. Duraiswami, NA Gumerov, and L. Davis, “Improved fast gauss transform and efficient kernel density estimation,” Computer Vision, 2003. Proceedings. Ninth IEEE International Conference on, pp. 664–671, 2003.

[8] H. Gou, A. Swaminathan, and M. Wu, “Noise features for image tampering detection and steganalysis,” in Proc. IEEE Int. Conf. Image Processing, San Antonio, TX, 2007, vol. 6, pp. 97–100.

[9] A. Swaminathan, M. Wu, and K. J. R. Liu, “Digital image forensics via intrinsic fingerprints,” IEEE Trans. Inform. Forensics Security, vol. 3, no. 1, pp. 101–117, 2008.

[10] A. C. Popescu and H. Farid, “Exposing digital forgeries in color filter array interpolated images,” IEEE Trans. Signal Processing, vol. 53, no. 10, pp. 3948–3959, 2005.

[11] B. E. Bayer, .Color imaging array,. US Patent, 3971065, 1976.

[12] H. Farid, “Digital image ballistics from JPEG quantization,” Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2006- 583, 2006.

[13] H. Farid, “Digital ballistics from jpeg quantization: A follow up study,” Dept. Comp. Sci., Dartmouth College, Tech. Rep. TR2008-638, 2008.

[14] Z. Fan and R. L. de Queiroz, “Identification of bitmap compression history: JPEG detection and quantizer estimation,” IEEE Trans. Image Process., vol. 12, no. 2, pp. 230–235, 2003.

[15] J. Lukas and J. Fridrich, “Estimation of primary quantization matrix in double compressed JPEG images,” in Proc. Digital Forensic Research Workshop, Cleveland, OH, Aug. 2003.

[16] A. C. Popescu and H. Farid, “Statistical tools for digital forensics,” in Proc. 6th Int. Workshop on Information Hiding, Toronto, Canada, 2004, pp. 128–147.

[17] W. Luo, Z. Qu, J. Huang, and G. Qiu, “A novel method for detecting cropped and recompressed image block,” in Proc. IEEE Conf. Acoustics, Speech and Signal.

[18] S. Ye, Q. Sun, and E. C. Chang, “Detecting digital image forgeries by measuring inconsistencies of blocking artifact,” in Proc. IEEE Int. Conf. Multimedia and Expo, Beijing, China, 2007, pp. 12–15.

[19] M. K. Johnson and H. Farid, “Detecting photographic composites of people,” in Proc. 6th Int. Workshop on Digital Watermarking, Guangzhou, China, 2007.

[20] M. K. Johnson and H. Farid, “Metric measurements on a plane from a single image,” Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2006-579, 2006.

[21] P. Nillius and J.-O. Eklundh, “Automatic estimation of the projected light source direction,” in Proc. IEEE Conf. Computer Vision and Pattern Recognition, 2001, pp. 1076–1083.

AUTHORS PROFILE

Sonal Patil has completed her B.E. M.Tech in CSE and pursuing PhD in Computer Engineering from S.V.N.I.T., Surat. She is working on Image forgery under valuable guidance of Dr. K.N. Jariwala. She has published papers on image forgery.

Dr. Krupa N. Jariwala has completed her B.Tech., M.Tech and PhD in Computer Engineering. She is Assistant Professor in Computer Engineering Department, S.V.N.I.T., Surat. Her research areas are Computer Vision, Image Processing, and Computer Network. She is having good number of publications on those research areas.