International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S, August 2019

A Technique to Detect Copy-Move Forgery using Enhanced SURF

Payal Srivastava, Manoj Kumar, Vikas Deep, Purushottam Sharma

Abstract*: *The field of digital imaging has advanced in recent years with increase of various digital gadgets and applications associated to it. With easily availability of image editing softwares which are either free of cost or budget friendly, image can be effortlessly tampered by the means of making forgery. This has led to increase in crime related to various image processing and computer vision applications. To combat with such forgeries digital forensic provide scientific techniques to identify whether image is original or forged. The proposed work implemented a image forgery check system based on SURF features. This is a pixel based technique where after preprocessing the images, relevant features are extracted and compared with a defined estimated threshold value. Based on the demonstrated results it is decided whether the image has been forged or not and if it is, then the area where tampering has been done is displayed as a forged part. The proposed algorithm is tested using open source CASIA image dataset. Also, the presented result shows that SURF feature based authentication provide forgery detection accuracy of 97%. The results are compared with other techniques in similar domain to prove the novelty of the work.

Keywords: Image Tampering, Forgery Detection, Advanced SURF, Copy-Move Forgery.

I. INTRODUCTION

The rapid development and research in various field of technologies have led to implementation of those ideas which was only imagined by people some decades ago. This helped in improving the lifestyle of people, increasing the performance of any work and reducing the time to complete any work. One such area is the digitization of media. From the time where people used reel camera, when they had to wait for some time for the photographs to be processed to the current scenario where a photo or video is instantly captured and processed to a final image; technology has come so far in this field. There are various software available in the digital market which helps people to modify a digital image if it is not as per their expectation. With the help of these softwares one can cut, edit and copy an object or Photoshop as per requirements. However, as every coin has two sides, this thing is also not an exception. While misusing these technologies, various fields ranging from the fashion industry to journalism, political campaigns to copyright of the research work and many provoking images which are mostly forged and edited are emerging in alarming frequency, thus questioning the integrity and validity of the digital images [1]. Also, if the fake or manipulated images are used as a proof in organizations it may lead to false judgments and hence injustice will be served [2]. Therefore, it is highly required to provide a highly accurate technique which will help to identify whether the digital image is forged or original. The techniques of digital forensics are broadly classified into five categories as shown below.

- Pixel based - To detect image anomalies at pixel level.
- Format Based - To compare statistical correlations using specific lossy compression scheme.
- Camera Based - To study and perform techniques on the images clicked by different brands of camera.
- Physics based - To detect anomalies between the objects in the three dimensional perspective.
- Geometric based - To study the position of the object with respect to the camera lens.

The objective of this work is to provide such a novel technique to prove the authenticity of digital images by finding copy-move based image forgeries. Since a single technique does not always guarantee the desired results, we suggested to make the technique more foolproof by proposing more powerful threshold based SURF. Hence, the proposed solution to the given problem is effective for finding image forgeries. In this domain, there are many ways to perform image forgery detection. A sample of copy-move forgery is shown in Figure 1.

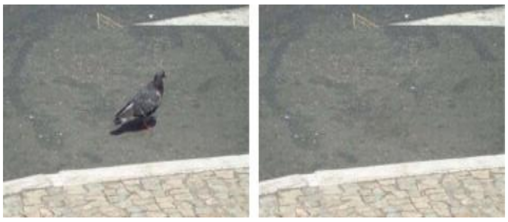

Figure 1. A sample image of copy-move based forgery. Left side image is original while the right side is a forged one

The paper is divided into five sections. Section 2 discusses the related work in this filed. The proposed method working is shown in Section 3 followed by results discussion in Section 4. Finally in Section 5, this work is concluded ith future scope.

Manuscript published on 30 August 2019.
***** Correspondence Author (s)

Payal Srivastava*, Department of Information Technology (ASET), AMITY University, Noida. Email: srivastavapayal28@gmail.com
Manoj Kumar, Department of Computer Science (ASET), AMITY University, Noida. Email: wss.manojkumar@gmail.com
Vikas Deep, Department of Information Technology (ASET), AMITY University, Noida. Email: vikasdeep8@gmail.com
Purushottam Sharma, Department of Information Technology (ASET), AMITY University, Noida. Email: psharma5@amity.edu

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

II. LITERATURE WORK

The growth of research and development in the field of digital forensics is advanced since approximately couple of decades. That was the time when various crimes related to forgery, modification of data in computer and copyright issues started cropping in. Various laws were sanctioned to punish the culprits behind these crimes; however, it was easier said than done to prove that the crime has been committed. Hence, it became necessary to invest in the field of digital forensics, especially related to copyright misuse and data authentication. There exist some techniques which assume that there are some underlying statistics changes while an image is forged, thus these changes can be used to detect the forgery. When somebody tries to change an image, certain inconsistencies are brought into the image and these can be uses to distinguish the altering. Two of the common pixel based techniques used for image forgery are [1].

1. Copy move based forgery - In which some part of the image is copied and pasted on another segment of the same image.
2. Image Splicing - In which an object from the same or another image is copied and pasted on the image.

Apart from pixel based techniques, the other techniques used currently in the field of digital forensics are based on the physics and geometry based assessments. Since, it is a known fact that images are taken under different lighting conditions [3]. Suppose, an image is clicked where a boy is playing football, and another image is clicked where a girl is jumping on joy. Further by using image splicing, a new image is created where the boy is playing football while that girl is behind that boy jumping. Looking at the image for the first time, one can easily judge that the girl is cheering for the boy. However, this is not true. But, by assessing the differences in the lighting condition on the girl as well as on boy, one can prove that there has been splicing done on the produced image. Also, if any manipulation is done on an image, there should be some change in the ‘fingerprints’ of that image, the differences in those fingerprints leads to proving the authenticity and integrity of that image. The example of fingerprints could be chromatic aberration, bicoherence, Camera Response Function (CRF) and JPEG quantization using which tampering can be detected via inconsistencies in these evidences of the original image and the image claimed to be forged [4]. The pixel based techniques are less complex compared to physics based forgery detection approaches. Some of the techniques based on template matching are proposed for forgery detection. These techniques detect tampering with respect to the original image by estimating the differences in pixels for both the images. The primary objective of these technique is to find a patch which matches in a given image. In this section mainly the work done using pixel based approaches are presented.

Amerini et al. [5] proposed a method to detect clone areas of an image. They used SIFT features and detected area of the mage where cloning is been performed. They recovered the parameters of geometric transformation as well. Their results are powerful in terms of forgery detection. Mishra et al. [6] suggested a copy move forgery detection technique based on SURF (speed up robust features) and hierarchical aglomerative clustering (HAC). They detected keypoints abd their neighbors using SURF and further grouping of these keypoints is done using HAC. The final results shows the copied region from the image based on grouping parameters. Li et al. [7] proposed a method to detect copy move forgery based on the key points based comparison. Their technique first segments the input image into semantically isolated image patches prior to key points extraction. Further they performed the key points matching using two stages. In the first stage, they find suspicious pair of patches that have copy move region and estimated an affine transformation matrix. In second step, they used EM (Expectation Maximization) to improve the estimated matrix which further confirm the copy move based forgery. Their experimental results are good in terms of forgery detection. Cozzolino et al. [8] suggested a new algorithm for copy move forgery detection and localization. Their approach is based on the computation of dense nearest neighbor search using the patch match randomized algorithm. Their experimental results shows high accuracy and speed in terms of forgery detection. Zhu et al. [9] proposed an approach based on SIFT (scale invariant feature transformation) key points and ORB features. They finds the Gaussian scale space followed by feature selections. The estimated ORB features in each scale space and matched these features with every two different key points using hamming distance and finally removes the false matched points using RANSAC algorithm. Their experimental results are robust against geometrical transformations. Yang et al. [10] presented a novel approach based on key points based analysis. They used SIFT based detector to find the key points for copy move forgery detection. An efficient key-points distribution based method is designed for intersecting the key points evenly for entire image and finally the key points are descripted for forgery detection. Their results confirms the accuracy. Hayat and Qazi [11] proposed a method which depends on discrete wavelet transform (DWT) and discrete cosine transform (DCT) for feature reduction. They first obtained the DWT image blocks and further the DCT is applied on these blocks. These blocks are then compared based on their correlation coefficients. To estimate the detection method a mask-based tampering approach is designed. Their results are better compared to other similar kind of techniques. Huh et al. [12] proposed a learning based algorithm to detect visual image manipulations. Their algorithm use EXIF metadata to train the model which checks the images self-consistency. This is further used detecting and localizing the image splices. Their technique is effective against various image forensic benchmarks.

All the techniques proposed in the literature have their own drawback and importance. But there exist no such technique which is highly accurate in terms of forgery detection accuracy and at the same time is applicable to detect forgery using multiple checks. The proposed work is an effort to improve the pixel based forgery detection by providing an advanced SURF based authentication check.

III. METHODOLOGY

A forged image is given as input for finding the traces of forged areas using proposed image authentication system. An advanced SURF algorithm is suggested to check the integrity of images. The proposed procedure works with 4 blocks of the image which are automatically chosen. Given the image which has been tampered and/or the claimed original image, the proposed generalized algorithm is shown below. The preprocessing of the image include conversion of the colored image into grayscale version and resizing the image into 512×512 pixels.

1.1 Proposed Advanced Speed up Robust Feature (SURF) Method

Speed up Robust Feature (SURF) is an advanced version of Scale Invariant Feature Transform (SIFT) algorithm. It was presented Bay et al. in 2006 [13], several times faster than the SIFT algorithm [14] and used mainly for applications such as object recognition, image classification etc. The SURF feature extraction algorithm is suggested in this work to determine copy move forgery. To implement the same, the image after preprocessing is divided into 4 blocks automatically. SURF generates Hessian matrix based unique scale and rotation-invariant interest point descriptor and detector. Here, we are extracting SURF feature (key) points for each block considered from an image. The algorithm of modified SURF in the proposed work is as follow:

- Convert the colored image into grayscale image.
- Resize the image into 512×512 pixels.
- Divide the image pixels into four blocks.
- Apply Equation 1 to compute matching key points:

$$\begin{aligned}
&Let\ i\ =\ First\ Block\ to\ be\ compared\\
&j\ =\ Second\ Block\ to\ be\ compared\\
&k\ =\ Position\ of\ the\ pixel\ in\ both\ the\ blocks\ i\ and\ j\\
&Where\ i\ \neq\ j\\
&S_{ik}\ =\ SURF(function)\ feature\ extracted\ from\ pixel\ k\ in\ block\ i\\
&S_{jk}\ =\ SURF(function)\ feature\ extracted\ from\ pixel\ k\ in\ block\ j\\
&compute\ M_{ij} = (M_{ij}+1) \quad \forall (S_{ik} = S_{jk})
\end{aligned}$$

(1)

The result of the images between all distinct blocks is to be observed for around 100-120 images from CASIA [15] image dataset. Based on the data evaluated, the threshold of matching points between the blocks is to be defined. The threshold is the minimum value of matching points M_{ij} which upon exceeding, is to be declared as copy move forgery between two blocks and the blocks are further displayed. Lastly, the approximate matching is used for finding the forgery. The representation of this algorithm is shown in Figure 2.

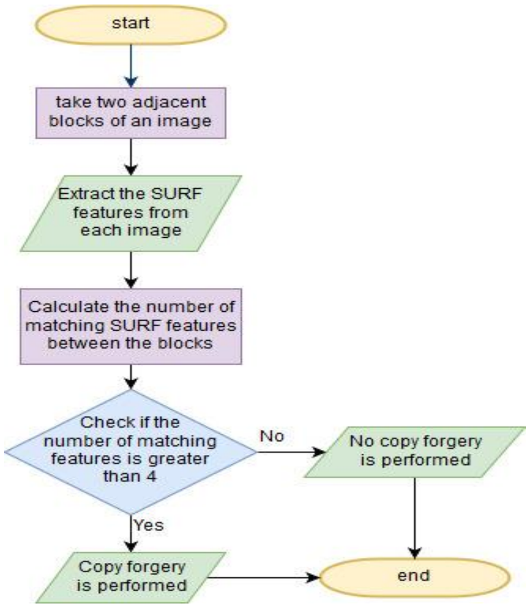
start
take two adjacent blocks of an image
Extract the SURF features from each image
Calculate the number of matching SURF features between the blocks
Check if the number of matching features is greater than 4
No
No copy forgery is performed
Yes
Copy forgery is performed
end

Fig.2. Flow chart of proposed SURF feature extraction algorithm

Here again, the algorithm is applied on various images of CASIA dataset to estimate the values of T_i for each image blocks so that a threshold shall be determined. If the value of T_i exceeds the threshold, then it will be inferred that image splicing is present in that i.e. i^{th} block of image P . Therefore, as a result, the final internal calculations for various blocks are done using below shown equations.
Let T_{hs} is the threshold value for SURF. Using the Equation 1 and estimated T_i value, the used threshold values are represented as:

$$T_{hs} = M_{ij} \quad \forall 0 < i < 4 \& 0 < j < 4 \quad \text{where } i \neq j$$

After calculating the threshold values, the forged blocks should be verified using below shown Equation 2 for proposed method.

$$M_{ij} > T_{hs} \qquad \forall 0 < i < 4 \& 0 < j < 4$$

(2)

And finally, after estimation of M_{ij} and T_i for all the blocks, they can be mapped with each other so that block forgeries can be verified.

IV. RESULTS

The proposed SURF feature extraction approach extract the features from each block of the image and compared them with each block. For example, the comparison is done between block 1 and 2, 1 and 3, 1 and 4, 2 and 3 and so on till all the blocks are compared with each other in an incremental fashion. Based on the results obtained from various CASIA dataset images, the estimated threshold value T_{hs} is 2.

It is found that using Equation 2, if the matching points M_{ij} between blocks i and j has value greater than 2 means there are the traces of copy move forgery. A sample of results obtained from various stages of the algorithm is shown in Figure 5 and Figure 6 where the image is divided into four blocks while Figure 7 shows the forgery in between the image blocks. This clearly states that using the modified SURF algorithm, we are able to identify the forgery between various blocks of the input image. Using Equation 7, we estimated $M_{ij} = 0$ for all $0 < i, j < 4$ and the values are less than T_{hs} therefore Figure 5 image is verified as original image while for Figure 6 we estimated $M_{34} = 31$ for all $0 < i < 4$ and $0 < j < 4$ which is greater than T_{hs} means a tampered image. There are total 31 matching points between both the blocks which justifies forgery in image.

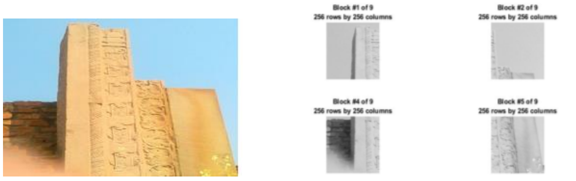

Fig.5. Original Input image and respective four image blocks

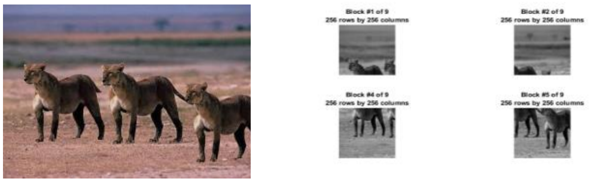

Fig.6. Copy-move forged image and respective blocks after preprocessing

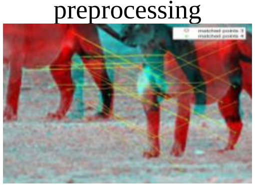

Fig.7. Forgery detected between 3rd and 4th block of image used in Figure 5

Another example of forgery detection is shown in Figure 8 with its proof in Figure 9. In this image the copy- move forgery done between block number 1 and 3 with a total of 14 matching points between both the blocks. As shown in the legends embedded in both figures (upper corners), the 'o' symbol denote matching points taken from the former blocks (3 and 1 in our cases) and the '+' symbol denote matching points taken from the latter blocks (4 and 3). These matching points 'o' and '+' taken from both the blocks are then mapped and represented using the yellow line in the figure.

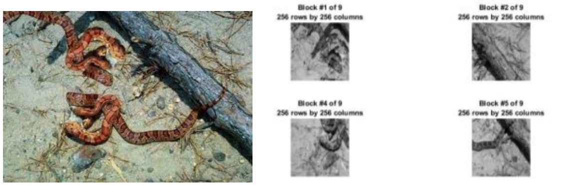

Fig.8. Input image and obtained blocks

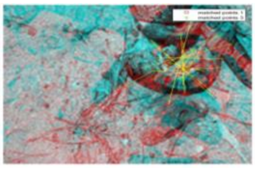

Fig.9. Forgery detected between 1st and 3rd block

To measure the performance of the above implemented algorithm, we calculated precision and recall as the probability of a detected forged image and later the probability of a truly forged image being detected as forged. Also, accuracy is defined as the probability of the images being detected correctly. This is achieved using below shown Equations.

$$precision = F \big/ (F + OF) \tag{9}$$

$$\mathrm{Re}\,call = F \big/ (F + FO) \tag{10}$$

$$Accuracy = (\mathrm{F} + O) \big/ (Total\ image\ tested) \tag{11}$$

Here, F represents forged image detected correctly, O represents original image detected correctly, FO is pertaining to forged image detected as original and OF is the original image detected as forged. Applying this on CASIA image data and comparing the results with similar kind of SURF algorithms in this domain, we obtained better results. The demonstrated results are shown in Table 1 which shows that proposed approach precision is 100% and accuracy is 98% compared with other approaches.

Table 1. Performance comparison of various surf algorithms

Method	T_{hs}	**Recall %**	**Accuracy%**	**Precision %**
SURF [16]	2.8	50	N/A	92.31
owSURF[14]	2.2	100	N/A	96
SURF [17]	-	97.27	97.27	97.27
SURF-HOG [17]	-	99.09	97.72	96.46
Proposed	2	87.5	98	100

V. CONCLUSION AND FUTURE WORK

In the proposed paper, an image forgery detection method is proposed using the threshold based advanced SURF feature extraction approach. The SURF feature method is used to detect location of copy move forgery within images. By testing with images of CASIA, it is found that the blocks in the images have forged data and the proposed SURF finds matching points more than or equal to 2.

After evaluating various images it is observed that the corresponding blocks each from both images having pixel difference of more than 40000 and is forged. In future work, we will try to identify the algorithm which will be able to identify which block in the image is original and which is fake using multi-way authentication system. We might be collaborating the Hough Transformation algorithm with the proposed method in order to accomplish this aim and improve the present algorithm to greater extent.

REFERENCES

1. H. Farid, "Image forgery detection," IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16-25, 2009.
2. M. Kumar and S. Srivastava, "Image forgery detection based on physics and pixels: a study," Australian Journal of Forensic Sciences, vol. 51, no. 2, pp. 119-134, 2019.
3. M. Kumar and S. Srivastava, "Image Tampering Detection Based on Inherent Lighting Fingerprints," in In: Hemanth D., Smys S. (eds) Computational Vision and Bio Inspired Computing. Lecture Notes in Computational Vision and Biomechanics, vol 28. Springer, Cham, 2018.
4. M. Kumar and S. Srivastava, "Image authentication by assessing manipulations using illumination," Multimedia Tools and Applications, vol. 78, no. 9, p. 12451–12463, 2019.
5. I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo and G. Serra, "Geometric tampering estimation by means of a SIFT-based forensic analysis," in IEEE International Conference on Acoustics, Speech and Signal Processing, Dallas, TX, USA , 2010.
6. P. Mishra, N. Mishra, S. Sharma and R. Patel, "Region Duplication Forgery Detection Technique Based on SURF and HAC," The Scientific World Journal, vol. DOI: http://dx.doi.org/10.1155/2013/267691, pp. 1-8, 2013.
7. J. Li, X. Li, B. Yang and X. Sun, "Segmentation-Based Image Copy-MoveForgery Detection Scheme," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 10, no. 3, pp. 507-518, 2015.
8. D. Cozzolino, G. Poggi and L. Verdoliva, "COPY-MOVE Forgery Detection basdon Patchmatch," in IEEE International Conference on Image Processing (ICIP), Paris, France, 2014.
9. Y. Zhu, X. Shen and H. Chen, "Copy-move forgery detection based on scaled ORB," Multimedia Tools and Applications, vol. 75, no. 6, p. 3221–3233, 2016.
10. B. Yang, X. Sun, H. Guo, Z. Xia and X. Chen, "A copy-move forgery detection method based on CMFD-SIFT," Multimedia Tools and Applications, vol. 77, no. 1, p. 837–855, 2018.
11. K. Hayat and T. Qazi, "Forgery detection in digital images via discrete wavelet and discrete cosine transforms," Computers & Electrical Engineering, vol. 62, pp. 448-458, 2017.
12. M. Huh, A. Liu, A. Owens and A. A. Efros, "Fighting Fake News: Image Splice Detectionvia Learned Self-Consistency," in European Conference on Computer Vision, Munich, Germany, 2018.
13. H. Bay, T. Tuytelaars and L. V. Gool, "SURF: Speeded Up Robust Features," in In: Leonardis A., Bischof H., Pinz A. (eds) Computer Vision – ECCV 2006. ECCV 2006. Lecture Notes in Computer Science, vol 3951, Springer, Berlin, Heidelberg, 2006.
14. D. Mistry and A. Banerjee, "Comparison of Feature Detection and Matching Approaches: SIFT and SURF," GRD Journals- Global Research and Development Journal for Engineering, vol. 2, no. 4, pp. 7-13, 2017.
15. W. W. Dong J, 2009–2017. [Online]. Available: http://forensics.idealtest.org/casiav1/join/. [Accessed 12 Auguest 2017].
16. J. Gong and J. Guo, "Image copy-move forgery detection using SURF in opponent color space," Transactions of Tianjin University, vol. 22, no. 2, pp. 151-157, 2016.
17. S. Prasad and B. Ramkumar, "Passive copy-move forgery detection using SIFT, HOG and SURF features," in IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India , 2016.

Retrieval Number: F11330886S19/2019©BEIESP
DOI:10.35940/ijeat.F1133.0886S19
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.