Detection of Image Forgery Using Speed Up Robust Technique

Dr. Swapan Debbarma,
Assistant Professor, Department of CSE,
NIT Agartala, Jirania, Tripura.

Poonam Chandel
Assistant Professor of Political Science,
Govt College Dhami, at 16 Mile , Shimla, and Research Scholar in Himachal Pradesh University .

Abstract: Tampering of images is one of the issues affecting our daily life and has greatly eroded the trust one use to have on photos. One of the most common types of image tampering is the copy-move forgery where part of the image is copied and paste in the same image. This is done with a motive to either highlight a particular object or to hide or remove an object from the image. Key points based approach uses descriptors from specific areas on the image unlike block based methods where features are extracted from every blocks. This lead to a smaller number of descriptors and hence a faster detection algorithm can be devised using key points. There are number of keypoints detection algorithms available such as SIFT, SURF, GLOH etc., in this paper we are using SURF for the purpose of feature extraction and forgery detection. We also analyse its performance in terms of speed and accuracy. Multiple cloning of region is also taken care of using iterative method in matching.

IndexTerms – Digital Forensic, Copy-move, SURF, Laplacian of Gaussian

I. Introduction

Tampering of digital images for vested interest is on a rise mainly due to easy availability of cheap digital camera along with sophisticated image editing software such as Adobe Photoshop, GIMP etc. Image forgery is seen in all area of our life, from fabricated insurance claim to scientific fraud, from magazine cover to false propaganda, from defamation to newspaper, images are no longer displaying the truth. Among the various type of image forgery [1] [2], cloning a part of the image is the most common method. This is done by copying a part of the image and then pasting it into another area of the same image, sometime pasting is done multiple times. Here the main motive is to either highlight a particular object in the image such as a crowd, or to hide or remove an object for instance, to conceal a person. When this is done properly using retouching tools, it can be very difficult to detect cloning. Moreover, since the copied points are from the same image, some components (eg, noise and color) will be compatible with the rest of the image and thus will not be detectable using methods that looks for incompatibilities in statistical measures in different part of the image. Detection becomes more difficult if the copied area is geometrically transformed before pasting. An example is shown in fig.1, where part of the image i.e., the leaves is copied in this case and paste onto the second truck, thus effectively removing it from the scene.

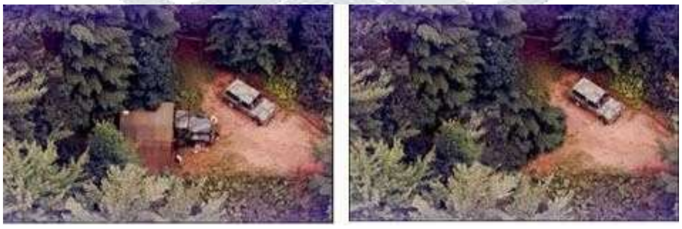


Fig.1. Example of image tampering

Detection of such copy-move forgery [3] is broadly categorized as block-based or key points-based, depending on the approach used. In the block-based approach, the image is divided into overlapping blocks. Then features are extracted from each blocks based on the techniques used such as DCT [3], PCA [4], SVD [5], Moments [6], etc. These features are then matched to detect similar blocks in the image. On the other hand, key point based forgery detection uses key points instead of blocks and since the number of key points in an image is extremely smaller than number of blocks, the computational requirement is quite low. In this paper we use a popular algorithm for the key point detection, Speed Up Robust Feature (SURF) [7] and we analyzed its performance in forgery detection in term of speed and accuracy.

The rest of the paper is organized as follows: Section 2 presents the review of the SURF algorithms; Section 3 describes the proposed methods for forgery detection. The result of the analysis is presented in Section 4 and Section 5 describes the conclusion of the paper.

II.Review of the Algorithms

A. Speed Up Robust Feature (SURF)

The SURF detector is based on integral image and Hessian matrix approximation [9]. The performance of SURF algorithm is much attributed to the use of an intermediate image representation known as the "Integral Image". The entry of an integral image $I_\Sigma(\mathbf{x})$ at a location $\mathbf{x}=(x,y)$ represents the sum of all pixels in the input image I within a rectangular region formed by the origin and **x**.

$$\sum_{i=0}^{i\le x}\sum_{j=0}^{j\le y} I(i,j) \qquad (4)$$

Once the integral image has been computed, it takes three additions to calculate the sum of the intensities over any upright, rectangular area. Hence, the calculation time is dependent of its size

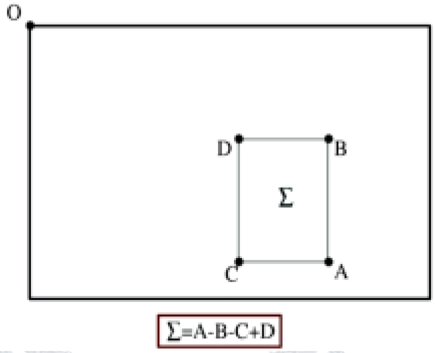


Fig.2. Integral image calculation by rectangular region

Given a point $\mathbf{x} = (x,y)$ in an image I, the Hessian matrix H(x,σ) in **x** at scale σ is defined as follows

$$H(x,\sigma) = \begin{bmatrix} Lxx(x,\sigma) & Lxy(x,\sigma) \\ Lxy(x,\sigma) & Lyy(x,\sigma) \end{bmatrix} \qquad (5)$$

where $L_{xx}(x, \sigma)$ is the convolution of the Gaussian second order derivative $\frac{\partial^2}{\partial x^2}$ g(σ) with the image I in the point x, and similarly for $L_{xy}(x, \sigma)$ and $L_{yy}(x, \sigma)$. These derivatives are called Laplacian of Gaussian. The approximate determinant of the Hessian matrix is calculated by

$$\det(H_{approx}) = D_{xx}D_{yy} - (0.9D_{xy})^2 \qquad (6)$$

1) *Orientation Assignment :* At first, a circular are is constructed around the keypoints. Then, Haar wavelets are used for the orientation assignment. It also increases the robustnes and decrease the computational cost. Haar wavelets are filters that detect the gradients in x and y directions. In order to make rotation invariant, a reproducible orientation for the interest point is identified. A circle segment of 60 is rotated around the interest point. The maximum value is chosen as a dominant orientation for that particular point.

2) *Feature descriptor Generation:* For generating the descriptors, first construct a square region around an interest point, where interest point is taken as the center point. This Square area is again divided into 4 smaller subareas. For each of these cells, Haar wavelet responses are calculated. Here, d_x termed as horizontal response and d_y as vertical response. For each of these subregions, 4 responses are collected as

$$v_{subregion} = [\sum dx, \sum dy, \sum|dx|, \sum|dy|,] \qquad (7)$$

So each subregion contributes 4 values. Therefore, the descriptor is calculated as 4X4X4=64. An example of SURF descriptors is shown in fig.3.

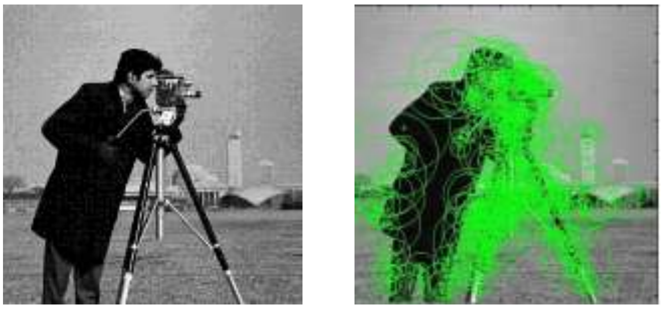


Fig. 3. Example of SURF key points

III. MATERIAL AND METHOD

In this section we describe in details the proposed method to detect duplicated and tampered area in an image. The input image is first converted into gray scale. Then keypoints as well as feature vectors are extracted using SURF algorithm. The vector dimension is 64. The proposed approach is illustrated in fig 4.

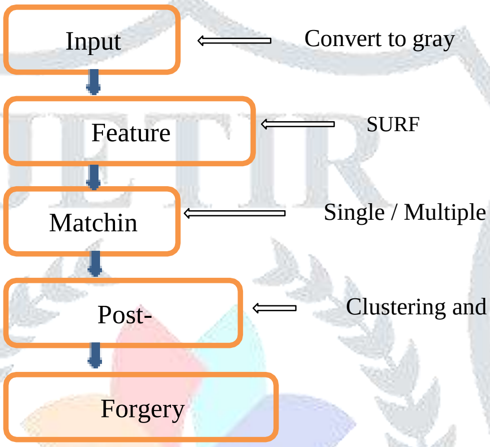


Fig.4. Overview of the Forgery Detection System

The extracted feature vector is matched differently for single clone detection and multiple cloning detection. For detecting single cloning, let $\mathbf{X} = \{x_1,..,x_n\}$ be a set of keypoints with the corresponding descriptors $\{f1,\ldots,f_n\}$. A matching operation is performed among the $\mathbf{f}_i$ vectors. The best candidate match for each keypoints x_i is found by identifying its nearest neighbor from all the other (n–1) keypoints of the image, which is the minimum Euclidean distance. The effective way is to use the ratio between the distances of the closest neighbor to that of the second-closest one, and comparing it with a threshold *T* (we fixed to 0.6). That is, the keypoint is matched only if

$$d_1 / d_2 < T \qquad (8)$$

where d_1 ,d_2 are the sorted Euclidean distances with respect to the other descriptors and $T \epsilon (0,1)$.

For detection of multiple cloning instead of checking the first two distances only, we iterate through all the adjacent distance pairs, i.e., the constraints can be given by

$$d_i / d_{i+1} < T \qquad (9)$$

where d_i are the sorted Euclidean distances with respect to the other descriptors and $T \epsilon (0,1)$.The image may contain very similar textures which may yield to false matches. These false matches can be reduced or eliminated to a great extent by performing post-processing on the matched output. An effective way to reduce false matches is to filter the output by using agglomerative hierarchical clustering [8]. The algorithm starts by assigning each keypoint to a cluster; then it computes all reciprocal spatial distances among clusters, find the closest pair of clusters, and finally merges them into a single cluster. This is repeated iteratively until a final merging situation is achieved through a linkage method adopted and by the threshold used to stop cluster grouping. In our experiment the threshold used is based on the distance criterion with cutoff value of 30. Single linkage is used for merging and creating a hierarchical tree and is given by

$$d(A,B) = \min (\mathrm{dist}(x_{Ai} ,y_{Bj})) \qquad (10)$$

This is nothing but the smallest Euclidean distance between objects in the two clusters.

IV.EXPERIMENTAL RESULTS

In this section, experiment of forgery detection is performed on the MICC-F220 dataset [9]. This dataset contains 220 images, and half of them are forged using a combination of different attacks such as scaling, rotation, blurring etc. We start by identifying the keypoints of the images using SURF. As given below in Table I, the average keypoints detected by SURF is only 880 compare to the average number of overlapping blocks needed in block based forgery detection approaches is 421692. This allows for a very low computational complexity in our method as compare to block based methods.

TABLE I:

AVERAGE KEYPOINTS DETECTED USING SURF AND AVERAGE NO OF 8X8 BLOCKS IN MICC F220 DATASET

Methods	Avg No. of Keypoints / blocks per image
SURF	880
Overlapping Blocks	421692

Following figures 5a to 5h shows the detection method in action. On the left we have the tampered image and the detected result is shown on the right. Figure 6 shows the profile summary indicating the running time of the processes.

Fig:5a

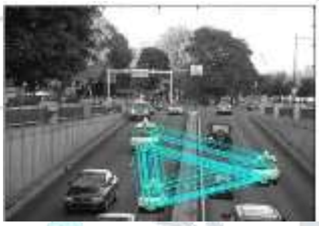


fig.:5b

fig: 5c

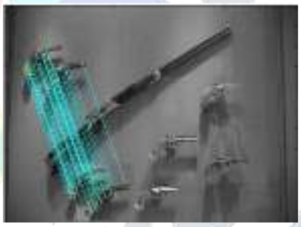


fig: 5d

fig: 5e

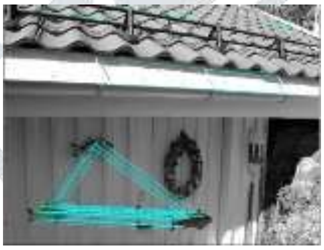


fig: 5f

fig: 5g

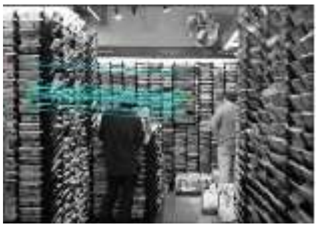
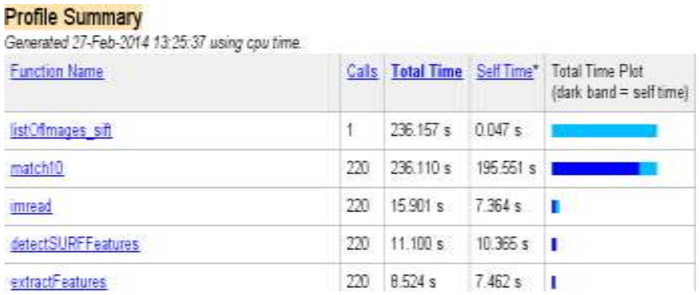


fig: 5h



Profile Summary

Generated 27-Feb-2014 13:25:37 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
listOfimages_sift	1	236.157 s	0.047 s	
match10	220	236.110 s	195.551 s	
imread	220	15.901 s	7.364 s	
detectSURFFeatures	220	11.100 s	10.365 s	
extractFeatures	220	8.524 s	7.462 s	

Fig.6. Running profile of SURF method, took 236 second to process 220 images

Detection performance was measured in terms of true positive rate (TPR) and false positive rate (FPR), where TPR is the fraction of the tampered images correctly identified as such, while FPR is the fraction of original images that are not correctly identified.

$$TPR = \frac{\#images\ detected\ as\ forged\ being\ forged}{\#forged\ images}$$

$$FPR = \frac{\#images\ detected\ as\ forged\ being\ original}{\#originalimages}$$

TABLE II:

TPR, FPR VALUES (%) AND PROCESSING TIME (AVERAGE PER IMAGE) FOR EACH METHOD

Methods	FPR%	TPR%	Time(s)
Fridrich et al.	84	89	294.69
Popescu and Farid	86	87	70.97
Amerini et al	8	100	4.94
SURF	5.45	88.18	1.02

The starting three rows shown in Table II are taken from [10-15] as a benchmark and the fourth row represents the values obtained from our SURF detection method. We see that SURF is extremely fast compared to other methods. On the other hand the TPR is lower than the rest.

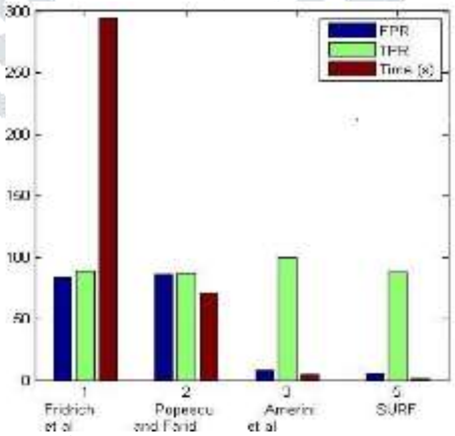


Fig.7. Performance of the methods represented in graph.

V.CONCLUSION

In this paper, key points based forgery detection is analyzed using SURF algorithm. The integral image used in SURF reduces the time complexities, which along with smaller feature dimension makes the detection extremely fast compare to other methods. Experimental results confirmed that the method is invariant towards different combination of scaling and rotation. They even give good results even in the presence of JPEG compression, Gaussian noise addition etc. The only drawback is the lack of key point detection in smooth or plain areas in the image.

REFERENCES

[1] H. Farid, “A survey of image forgery detection,” IEEE Signal Process. Mag., vol. 2, no. 26, pp. 16–25, 2009.

[2] S. Lyu and H. Farid, “How realistic is photorealistic?,” IEEE Trans. Signal Process., vol. 53, no. 2, pt. 2, pp. 845–850, Feb. 2005.

[3] J. Fridrich, D. Soukal, and J. Lukas. Detection of copy-move forgery in digital images. In Digital Forensic Research Workshop, 2003.

[4] A.C.Popescu and H.Farid, “Exposing digital forgeries by detecting duplicated image regions,” Dartmouth College, Hanover, New Hampshire, USA: TR2004-515, 2004.

[5] G.Li, Q.Wu, D.Tu, and Shaojie Sun, “A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD,” IEEE International Conference on Multimedia & Expo, 2007.

[6] Seung-Jin Ryu, Min-Jeong Lee and Heung-Kyu Lee,“Detection of Copy-Rotate-Move Forgery using Zernike Moments”, in: 12th International Workshop on Information Hiding, Calgary,Alberta, Candada, 2010

[7] Xu Bo,Wang Junwen, Liu Guangjie, Dai Yuewei, “Image Copy- Move Forgery Detection Based on SURF”, in Proceedings of the International Conference on Multimedia Information Networking and Security (MINES) pp. 889 -892, 2010

[8] T. Hastie, R. Tibshirani, and J. H. Friedman, The Elements of Statistical Learning. New York: Springer, 2003.

[9] http://www.micc.unifi.it/ballan/research/image-forensics/

[10] I. Amerini, L. Ballan, R. Caldelli, A. del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and tranformation recovery", *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, 2011

[11] Pradhan, M. C., Satpathy, S., & Bhoi, B. K. (2015, May). An improved FPGA based model for automatic traffic sign detection. In 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM) (pp. 291-298). IEEE.

[12] Pradhan, M. C., Satpathy, S., & Bhoi, B. K. (2016). An Intelligent Fuzzy Based Technique of Making Food Using Rice Cooker. Asian Journal of Electrical Sciences, 5(1), 1-7.

[13] Satpathy, S., Das, S., & Debbarma, S. (2019). Development a Novel Approach of Fuzzy Based FPGA System for Prediction of Jaundice in Rural Area. Journal of Engineering Technology (ISSN. 0747-9964), 8(1), 32-39.

[14] Sengupta, A. S., Satpathy, S., Mohanty, S. P., Baral, D., & Bhattacharyya, B. K. (2018). Supercapacitors Outperform Conventional Batteries [Energy and Security]. IEEE Consumer Electronics Magazine, 7(5), 50-53.

[15] Satpathy, S., & Sahu, A. P. (2015, December). A Graphical User Interface, Fuzzy Based Intelligent Rice Cooker. In 2015 International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 1216-1220). IEEE