

A Novel Technique for Detection of Copy Move Forgery Using MSER Features

Kanica Sachdev

Department of Computer Science, Model Institute of Engineering and Technology, Jammu, India

Abstract – Digital image forgery detection is one of the most significant fields in image forensics. It refers to the editing or alteration of the image contents. Since an image may be presented as a legal proof of evidence, thus verifying its originality is of utmost importance. Recent improvements in image capturing devices and image editing softwares have made the process of forging images simple. The most common type of image forgery is copy move forgery. In this, a part or block of an image is copied and then pasted on the same image. The pasted area may be scaled or rotated to make the process of forgery detection difficult. The proposed technique uses MSER features to detect forgery in images. MSER features are stable and invariant to affine transformations. They are used in a number of applications for blob detection. In the introduced method, the extracted MSER features from the image are matched to find the forged areas in the image. The matched points correctly identify the copied and pasted areas of the altered image. The proposed method even detects forgery in the presence of rotation and scaling of forged area. It is a low complexity algorithm that is shown to perform efficiently on standard dataset.

Index Terms – Digital images; image forensics; image forgery; copy move forgery; MSER features.

1. INTRODUCTION

In the existing times, digital images have completely replaced the analog images i.e. photographs. Since the digital images are easy to capture, store and access; they are being increasingly used in a variety of applications. However, the recent advances in the field of digital imaging have also posed a serious problem of image forgery. It refers to editing or manipulation of images in any form. Lately, many fake images are being identified in courtrooms, scientific journals, magazines etc [1]. The low price of the image capturing devices and the easy availability of numerous image editing softwares has certainly made the process of altering images easier. This has given rise to the field of image forensics in order to restore our faith in digital images. The most important element of image forensics is image forgery detection.

Image forgery detection refers to identifying fake or altered images to ensure their authenticity. Image forgery is broadly classified into three types: retouching, image splicing and copy move forgery. Image retouching, also known as airbrushing is altering an image imperceptibly so as to enhance it, like removing the wrinkles of a subject. It introduces minute changes in the image such as changing the brightness, or altering the

contrast. It is not considered to be as harmful as other types of image forgery. Image splicing is the formation of a fake image using regions of two or more images [2]. Many methods and techniques have been developed to detect image splicing using image features and camera features. The third and most common type of forgery is copy move forgery. It is performed by copying a region of an image and pasting it at some other location on the same image. It is relatively difficult to detect as the pasted segment has similar properties with the image and these properties cannot be used to distinguish the forged region from the original image [3]. Several techniques have been established to detect this type of forgery, which can be largely divided into block based techniques and keypoint based techniques. Block based techniques mainly divide the entire image into blocks or segments and use a certain feature to find blocks that are similar [4-14]. The similar blocks represent the copied and the forged areas. The block based methods are simple and accurate, however they are computationally expensive as they involve the calculation of features of each block and then comparing every pair of block to find duplicate regions. Also, they fail to identify forged regions in the presence of operations like rotation, scaling etc. This gave rise to the development of keypoint based methods. The keypoint based methods extract certain distinguishing points from the image and compare them to find the forged regions. Certain methods using a combination of both block based and keypoint based techniques have also been developed [15-17]. These methods have been discussed further.

Section 2 discusses the various existing keypoint based techniques for the detection of copy move forgery. Their results and drawbacks have also been explained briefly. Section 3 explains the proposed technique in detail. Section 4 mentions the particulars of the testing environment and the database used along with presenting the results of the proposed method. Section 5 summarizes the work and suggests future enhancements.

2. LITERATURE SURVEY

The keypoint based methods select certain high entropy regions from an image. The points are then localized and robust local descriptors are constructed from them. These keypoint descriptors are then compared to find the similar areas of an image [18]. The two types of keypoints that have been used to

detect forgery are SIFT (Scale Invariant Feature Transform) and SURF (Speeded Up Robust Features).

SIFT features were developed by David Lowe in 1999 [19]. They are used in a variety of applications like video tracking, object recognition, 3D modeling etc. The process of finding SIFT keypoints and their descriptors are divided into four main stages: detecting the scale-space extrema, localizing the detected point, assigning orientation and finding keypoint descriptor.

Many copy move forgery detection methods utilize SIFT keypoints. Huang et al., for instance, developed a method to detect forgery using SIFT [20]. These keypoints were matched by best bin first technique of nearest neighbor of the keypoints. This method was immune to scaling and rotation but was not very efficient. Another method was proposed by Ardizzone et al. [21] It involves three basic steps: clustering of the SIFT keypoints, matching of the keypoint clusters and lastly texture analysis. Although this method provided good results, the method failed when the number of clusters was too many or too few. A novel technique was proposed by Amerini et al. [22] It involved the calculation of SIFT keypoints and feature matching using the g2NN test. After this, the keypoint clusters were formed by agglomerative hierarchical clustering to find forged areas and geometric estimation was performed. The technique provided good results on the standard dataset MICC-F220. But it failed to detect forgery in an image that contains large uniform areas. Pan and Lyu proposed a technique that found and matched the SIFT keypoints to find tampered areas [23]. Further, the geometric distortions of the forged areas were deduced by random sample consensus (RANSAC). The method was immune to JPEG compression and addition of noise. Shivakumar and Baboo developed a method to identify tampering by using Harris points [24]. The descriptors of the points were found using SIFT algorithm and were matched. The method was faster as Harris point detection algorithm is faster than SIFT. Another novel approach was proposed by Kaur et al. [25] It utilized both DCT (Discrete Cosine Transform) and SIFT. Since DCT is immune to JPEG compression and addition of noise, the performance considerably improved.

SURF features have also been used for the detection of copy move forgery in images. SURF keypoints were proposed by Bay et al. in 1996 [26]. These features are considered to be faster than SIFT. The feature points are detected using box filters of different size which are convolved with the integral image to form the scale space. Hessian matrix is then used to find the potential keypoints. For orientation assignment, Haar wavelet responses at every point in a circular neighborhood are considered.

Many researchers have utilized SURF keypoints for the detection of image forgery. Bo, Junwen, Guangjie and Yuewei detected forgery using SURF keypoint matching [27].

Although the technique provided good results and was immune to scaling, rotation and blurring, it failed to detect the exact boundaries of the forged regions. Another method proposed by Shivakumar and Baboo used SURF keypoints and then verified whether the detected areas were forged [28]. It gave a very low false positive rate. Guang-qun Zhang and Hang-jun Wang also developed a method for identifying forged areas [29].

The image was first divided into flat and non flat regions. The forgery in flat regions was detected using Fourier-Mellin Transform (FMT) of image blocks. For the non flat areas, SURF keypoint matching was employed. Mishra et al. proposed a technique based on SURF keypoints and hierarchical agglomerative clustering (HAC) [30]. The SURF keypoints from the image were detected and matched to find similar areas. The ratio of distance between two nearest neighbor keypoints was considered for matching. After this, HAC was performed to eliminate false matchers and identify the keypoints that correctly indicate forged regions. Mohammad Hashmi et al also suggested a method that used SURF keypoints and wavelet transform [31]. The SURF points were detected from the wavelet transform of the image and then matched. The features become more predominant due to the wavelet domain.

Salma Amtullah and Ajay Koul used the nearest neighbor approach for matching the SURF keypoints [32]. The ratio of the nearest neighbor and the second nearest neighbor of the keypoint was compared to a threshold value to identify forgery. The method was invariant to compression, scaling, noise addition, rotation and blurring. It also detected multiple forgeries on the same image. Silva et al. suggested a novel method to detect image forgery using multiscale representation and voting processes [33]. The detected SURF keypoints are clustered using geometric constraints. For each scale of the image, the generated clusters are examined. A voting process is then carried out from the results at different scales to ascertain forgery.

A combination of keypoint detection methods is has also been used. Kumar et al. used SURF keypoint detection and then used Binary Robust Invariant Scalable Keypoints (BRISK) features for matching using knn searching method [34]. Similarly, Pandey et al. used both SIFT and SURF features to detect forgery [35]. This improved the accuracy considerably. They further refined their work by localizing the tampered areas by hybrid SIFT Histogram of Gradient (HOG) and SURF HOG features.

Although a lot of research has been done in the field of copy move image forgery detection; particularly using the keypoint based techniques. However, there is no single method that has been able to detect forgery on a standard database under all post processing operations and still has a low complexity. Thus, we can say that the research in the field of copy move forgery

detection of images is still at an initial phase and requires contributions from various researchers.

3. PROPOSED TECHNIQUE

The proposed method has been illustrated in Figure 1. The MSER features are first detected from the image. Successively, the descriptors of these keypoints are found. The ratio of the distances between the nearest neighbor and the second nearest neighbor of each keypoint is then matched to a threshold value for the process of matching. The matched keypoints represent the forged areas from the image.

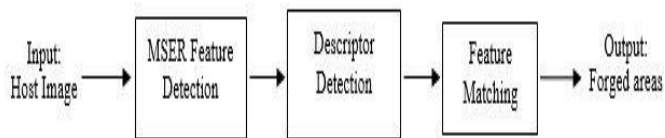


Fig. 1. Flowchart for the proposed method

A. MSER Feature Detection

Maximally stable extremal regions (MSER) keypoints have been proposed by Matas et al. in 2002 [36]. They were primarily used for blob detection and object recognition. MSER were used to find similar regions between two images that have been taken from two different perspectives. MSER keypoints are defined by the image intensity and the outer border of images. These keypoints offer various advantages over other types of keypoints. They are invariant to affine transformations and can also be used for multiscale detection. These points are also stable and remain constant over a range of thresholds [37]. The worst case complexity of extremal regions is $O(n)$, where n is the number of pixels [38]. Hence, it is a low complexity keypoint detection technique. MSER keypoints are also invariant to blurring, light change and scale change.

For a binary image I and threshold value t , MSER region E_t is defined as

$$E_t(x) = \begin{cases} 1, & \text{if } I(x) \geq t \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

To understand the concept of MSER, we consider all possible threshold values for a given image I . The intensity values of pixels below the threshold value t are black and above this threshold are white. If we watch the images with increasing values of threshold t in succession, we will initially see a white image. Thereafter, we will see certain black spots in regions of local minima which will keep growing subsequently. Ultimately, we will see a complete black image. Maximal regions can be formed by combining the set of connected components of all these individual images.

To enumerate the MSER features, the pixels are sorted in ascending order depending on their intensities. These are then

placed in the image and a list of the connected components and their respective areas is constructed using unionfind algorithm [39]. This produces a record of the areas of connected components as a function of intensity. Lastly, the local minima intensity points of rate of change of area function are chosen as the threshold points that represent the maximally stable extrema regions.

B. Descriptor Detection

The descriptors of the detected points are extracted using SURF descriptor detection. SURF descriptors have been used for tracking objects, recognizing objects or faces, 3D reconstruction etc. [40] The aim of a descriptor is to provide a robust and unique characterization to a keypoint. They represent the distribution of intensity within the neighboring pixels of the keypoint. To compute the descriptor, an orientation is assigned to the keypoint and then the descriptor is extracted from it.

- i) Orientation assignment: To assign an orientation to the keypoint. The Haar wavelet response within a neighboring area of 6×6 is calculated in the horizontal and vertical direction. The wavelet responses are then weighted using a Gaussian function around the point of interest in a two dimension coordinate system. The sum of all the wavelet responses is calculated to find a dominant orientation. An orientation vector is formed from these summed responses. The orientation of the keypoint is taken to be the longest such vector.
- ii) Calculating the descriptor: To find the descriptor, a square region is considered with the centre as the keypoint along the calculated orientation. The window size is taken as 20×20 . The interest region is then divided into smaller 4×4 sub regions and Haar wavelet responses are extracted at sample points. The computed responses are then weighted with a Gaussian function. This provides greater robustness against noise addition or deformations.

C. Keypoint Matching

The keypoints are then matched to find the forged areas using their descriptors. Most of the techniques use Euclidean distance for comparing the distance between the points. In this paper, cosine similarity has been used as the distance measure for comparison as it reduces the complexity and increases the speed. The comparison of distance between the keypoints to a global threshold value did not provide good results because of the high dimensional feature space. Hence, the 2NN technique for comparison of keypoints was developed [21]. According to this technique, the ratio of the nearest neighbor and the second nearest neighbor of the keypoint is compared with a threshold value. If the similarity vector $V = \{V_1, V_2, \dots, V_n\}$ represents the distances of the various other keypoints in sorted manner, then the keypoint is considered to be matched if

$$V_1/V_2 < z \quad (2)$$

TABLE I. DETAILS OF COMOFOD DATABASE

Description	
Camera for capturing	Canon EOS 7D Camera
Software for forging images	Photoshop CS3 and CS5
Dimension of images	The size of the captured images was 5202×3465 pixels which was later resized
Format	Portable Network Graphics (PNG)
Image Topic	Various

where z is the threshold value. Thus the matching process can be summarized as:

- Consider the keypoints found using MSER feature.
- Calculate the distance of the keypoint with all the other keypoints using cosine similarity to form a distance vector V . V contains the distance of the keypoint with all the other keypoints.
- Sort the distance vector V in ascending order.
- Calculate the ratio of the nearest neighbor and the second nearest neighbor i.e. V_1/V_2
- If the calculated ratio is less than threshold value (z), the points are considered to be matched. The threshold value has been set as 0.4 in the experiments.
- Repeat step ii) to v) for all the MSER keypoints.

Display the set of matched keypoints on the image to represent the original and the forged area.

4. RESULTS

The proposed method has been implemented and tested in Matlab environment. The standard database used for testing the technique is CoMoFoD [41]. It provides various semantically meaningful images that have been taken under different conditions that help to objectively evaluate the technique of forgery detection. The details of the database have been provided in Table I.

The results of proposed method have been shown in Fig. 2. Fig. 2 i-x) depict the original images. Fig. 2 xi-xx) show the forged images where copy move forgery have been applied to hide certain details or in order to duplicate items. Fig. 2 xxi-xxx) present the results of applying the algorithm proposed in this paper to detect forgery. The red lines in these images show the copied area and the corresponding pasted area. Fig. 2 xi-xii) show simple copy move forgery by translating a part of the image. Their corresponding detection results have been depicted in Fig. 2 xxi-xxii). Fig. 2 xiii-xiv) show forged images where the forged area has been rotated and then pasted on the image. Their detection is shown in Fig. 2 xxiii-xxiv). Fig. 2 xv-xvi) show forged images with scaling transformation of the copied area, Fig. 2 xvii-xviii) show tampered images with distortion of the copied area and Fig. 2 xix-xx) show forged images with a combination of transformations applied to the pasted area. Their respective detection results have been shown in Fig. 2 xxv-xxx).

As it is evident from the results, the proposed technique is able to detect copy move forgery efficiently even in the presence of geometrical transformations being applied to the forged area. The technique can detect forgery in the presence of scaling, rotation, distortion and even when a combination of these transformations is applied. Hence, the technique to detect copy move forgery based on MSER features presented in this paper is efficient and robust.

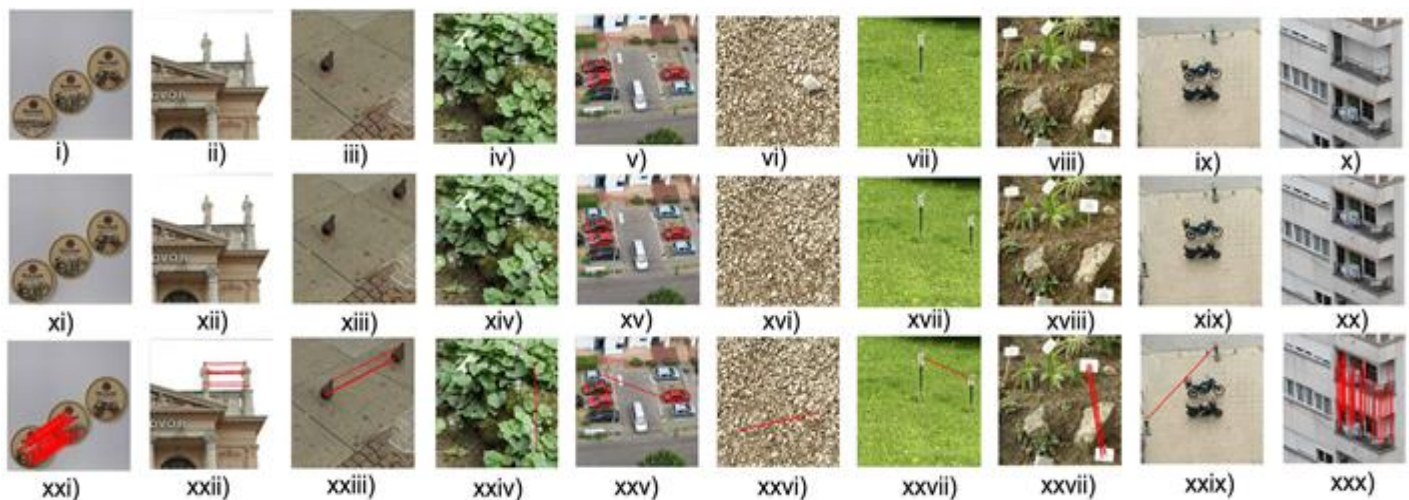


Fig. 2. Results of applying the proposed scheme on the database

5. CONCLUSION

This paper proposes a novel technique for the detection of copy move forgery. It is a low complexity technique that uses MSER keypoints to match the copied and the pasted regions. The descriptors of the MSER keypoints are matched using cosine similarity as the distance measure to find the tampered areas. The method is robust against various geometrical transformations i.e. scaling, rotation and distortion. It is also immune to a combination of these transformations. Future work can focus on decreasing the number of false negatives. It can also include the localization of the forged areas from the keypoints to show the exact copied and pasted regions.

REFERENCES

- [1] Farid, Hany. "Image forgery detection." *IEEE Signal processing magazine* 26, no. 2 (2009): 16-25.
- [2] Ng, T-T., and S-F. Chang. "A model for image splicing." In *Image Processing, 2004. ICIP'04. 2004 International Conference on*, vol. 2, pp. 1169-1172. IEEE, 2004.
- [3] Christlein, Vincent, Christian Riess, Johannes Jordan, Corinna Riess, and Elli Angelopoulou. "An evaluation of popular copy-move forgery detection approaches." *IEEE Transactions on information forensics and security* 7, no. 6 (2012): 1841-1854.
- [4] Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukáš. "Detection of copy-move forgery in digital images." in *Proceedings of Digital Forensic Research Workshop*. 2003.
- [5] Popescu, A. C., and H. Farid. "Exposing digital forgeries by detecting duplicated image region [Technical Report]. 2004-515." Hanover, Department of Computer Science, Dartmouth College. USA (2004).
- [6] Luo, Weiqi, Jiwu Huang, and Guoping Qiu. "Robust detection of region-duplication forgery in digital image." In *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, vol. 4, pp. 746-749. IEEE, 2006.
- [7] Mahdian, Babak, and Stanislav Saic. "Detection of copy-move forgery using a method based on blur moment invariants." *Forensic science international* 171, no. 2 (2007): 180-189.
- [8] Li, Guohui, Qiong Wu, Dan Tu, and Shaojie Sun. "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD." In *Multimedia and Expo, 2007 IEEE International Conference on*, pp. 1750-1753. IEEE, 2007.
- [9] Bashar, Md Khayrul, Keiji Noda, Noboru Ohnishi, Hiroaki Kudo, Tetsuya Matsumoto, and Yoshinori Takeuchi. "Wavelet-Based Multiresolution Features for Detecting Duplications in Images." In *MVA*, pp. 264-267. 2007.
- [10] Zhang, Jing, Zhanlei Feng, and Yuting Su. "A new approach for detecting copy-move forgery in digital images." In *Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on*, pp. 362-366. IEEE, 2008.
- [11] Bayram, Sevinc, Husrev Taha Sencar, and Nasir Memon. "An efficient and robust method for detecting copy-move forgery." In *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, pp. 1053-1056. IEEE, 2009.
- [12] Wang, Junwen, Guangjie Liu, Zhan Zhang, Yuewei Dai, and Zhiquan Wang. "Fast and robust forensics for image region-duplication forgery." *Acta Automatica Sinica* 35, no. 12 (2009): 1488-1495.
- [13] Wang, Junwen, Guangjie Liu, Hongyuan Li, Yuewei Dai, and Zhiquan Wang. "Detection of image region duplication forgery using model with circle block." In *2009 International Conference on Multimedia Information Networking and Security*, pp. 25-29. IEEE, 2009.
- [14] Ryu, Seung-Jin, Min-Jeong Lee, and Heung-Kyu Lee. "Detection of copy-rotate-move forgery using Zernike moments." In *Information Hiding*, pp. 51-65. Springer Berlin Heidelberg, 2010.
- [15] Pun, Chi-Man, Xiao-Chen Yuan, and Xiu-Li Bi. "Image forgery detection using adaptive oversegmentation and feature point matching." *Information Forensics and Security, IEEE Transactions on* 10, no. 8 (2015): 1705-1716.
- [16] Y. J. Peng and C. S. Fuh, "Segmentation-Based Image Copy-Move Forgery Detection Method with Consideration of Spatial Correlation," *Proceedings of IPPR Conference on Computer Vision, Graphics, and Image Processing*, Yilan, Taiwan, P2-4, Paper# 39, pp.1-8, 2015.
- [17] Sachdev, Kanika, Mandeep Kaur, and Savita Gupta. "A Robust and Fast Technique to Detect Copy Move Forgery in Digital Images Using SLIC Segmentation and SURF Keypoints." In *Proceeding of International Conference on Intelligent Communication, Control and Devices*, pp. 787-793. Springer Singapore, 2017.
- [18] Warbhe, Anil Dada, R. V. Dharaskar, and V. M. Thakare. "A Survey on Keypoint Based Copy-paste Forgery Detection Techniques." *Procedia Computer Science* 78 (2016): 61-67.
- [19] Lowe, David G. "Object recognition from local scale-invariant features." In *Computer vision, 1999. The proceedings of the seventh IEEE international conference on*, vol. 2, pp. 1150-1157. Ieee, 1999.
- [20] Huang, Hailing, Weiqiang Guo, and Yu Zhang. "Detection of copy-move forgery in digital images using SIFT algorithm." In *Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on*, vol. 2, pp. 272-276. IEEE, 2008.
- [21] Ardizzone, Edoardo, Alessandro Bruno, and Giuseppe Mazzola. "Copy-Move Forgery Detection by Matching Triangles of Keypoints." *Information Forensics and Security, IEEE Transactions on* 10, no. 10 (2015): 2084-2094.
- [22] Amerini, Irene, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra. "A sift-based forensic method for copy-move attack detection and transformation recovery." *Information Forensics and Security, IEEE Transactions on* 6, no. 3 (2011): 1099-1110.
- [23] Pan, Xunyu, and Siwei Lyu. "Detecting image region duplication using SIFT features." In *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*, pp. 1706-1709. IEEE, 2010.
- [24] Shivakumar, B. L., and S. Santhosh Baboo. "Automated forensic method for copy-move forgery detection based on Harris interest points and SIFT descriptors." *International Journal of Computer Applications* 27, no. 3 (2011): 9-17.
- [25] Kaur, Amanpreet, and Richa Sharma. "Copy-move forgery detection using DCT and SIFT." *International Journal of Computer Applications* 70, no. 7 (2013).
- [26] Bay, Herbert, Tinne Tuytelaars, and Luc Van Gool. "Surf: Speeded up robust features." In *Computer vision-ECCV 2006*, pp. 404-417. Springer Berlin Heidelberg, 2006.
- [27] Bo, Xu, Wang Junwen, Liu Guangjie, and Dai Yuewei. "Image copy-move forgery detection based on SURF." In *Multimedia information networking and security (MINES), 2010 international conference on*, pp. 889-892. IEEE, 2010.
- [28] Shivakumar, B. L., and Lt Dr S. Santhosh Baboo. "Detection of region duplication forgery in digital images using SURF." *IJCSI International Journal of Computer Science Issues* 8, no. 4 (2011).
- [29] Zhang, Guang-qun, and Hang-jun Wang. "SURF-based detection of copy-move forgery in flat region." *International Journal of Advancements in Computing Technology* 4, no. 17 (2012).
- [30] Mishra, Parul, Nishchol Mishra, Sanjeev Sharma, and Ravindra Patel. "Region duplication forgery detection technique based on SURF and HAC." *The Scientific World Journal* 13 (2013).
- [31] Hashmi, Mohammad Farukh, Vijay Anand, and Avinash G. Keskar. "A copy-move image forgery detection based on speeded up robust feature

- transform and Wavelet Transforms." In Computer and Communication Technology (ICCCT), 2014 International Conference on, pp. 147-152. IEEE, 2014.
- [32] Amtullah, Salma, and Ajay Koul. "Passive image forensic method to detect copy move forgery in digital images." *IOSR Journal of Computer Engineering (IOSR-JCE)* 16, no. 2 (2014): 96-104.
- [33] Silva, Ewerton, Tiago Carvalho, Anselmo Ferreira, and Anderson Rocha. "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes." *Journal of Visual Communication and Image Representation* 29 (2015): 16-32.
- [34] Kumar, Sunil, J. V. Desa, and Shaktidev Mukherjee. "A fast keypoint based hybrid method for copy move forgery detection." *arXiv preprint arXiv:1612.03989* (2016).
- [35] Pandey, Ramesh Chand, Rishabh Agrawal, Sanjay Kumar Singh, and Kaushal K. Shukla. "Passive Copy Move Forgery Detection Using SURF, HOG and SIFT Features." In *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)* 2014, pp. 659-666. Springer International Publishing, 2015.
- [36] Extremal, Maximally Stable, J. Matas, O. Chum, M. Urban, and T. Pajdla. "Robust wide baseline stereo from." In *British Machine Vision Conference*. 2002.
- [37] Donoser, Michael, and Horst Bischof. "Efficient maximally stable extremal region (MSER) tracking." In *Computer Vision and Pattern Recognition, 2006 IEEE Computer Society Conference on*, vol. 1, pp. 553-560. IEEE, 2006.
- [38] Nistér, David, and Henrik Stewénus. "Linear time maximally stable extremal regions." In *European Conference on Computer Vision*, pp. 183-196. Springer Berlin Heidelberg, 2008.
- [39] Monge, Alvaro, and Charles Elkan. "An efficient domain-independent algorithm for detecting approximately duplicate database records." (1997).
- [40] Bay, Herbert, Andreas Ess, Tinne Tuytelaars, and Luc Van Gool. "Speeded-up robust features (SURF)." *Computer vision and image understanding* 110, no. 3 (2008): 346-359.
- [41] Tralic, Dijana, Ivan Zupancic, Sonja Grgic, and Mislav Grgic. "CoMoFoD—New database for copy-move forgery detection." In *ELMAR, 2013 55th International Symposium*, pp. 49-54. IEEE, 2013.