International Journal on Future Revolution in Computer Science & Communication Engineering ISSN: 2454-4248
Volume: 7 Issue: 4 30 – 41

# Numerical Simulation and Design of Copy Move Image Forgery Detection Using ORB and K Means Algorithm

Aditya Atreya[a], Khushbu Garg[b]
[a]M. Tech. Scholar, Department of Computer Science & Engineering, RIET, Jaipur
[b]Assistant Professor, Department of Computer Science, RIET, Jaipur

**Abstract**
Copy-move is a common technique for tampering with images in the digital realm. Therefore, image security authentication is of critical importance in our society. So copy move forgery detection (CMFD) is activated in order to identify the forged portion of a photograph. A combination of the Scaled ORB and the k-means++ algorithm is used to identify this object. The first step is to identify the space on a pyramid scale, which is critical for the next step. A region's defining feature is critical to its detection. Because of this, the ORB descriptor plays an important role. Extracting FAST key points and ORB features from each scale space. The coordinates of the FAST key points have been reversed in relation to the original image. The ORB descriptors are now subjected to the k-means++ algorithm. Hammering distance is used to match the clustered features every two key points. Then, the forged key points are discovered. This information is used to draw two circles on the forged and original regions. Moment must be calculated if the forged region is rotational invariant. Geometric transformation (scaling and rotation) is possible in this method. For images that have been rotated and smoothed, this work demonstrates a method for detecting the forged region. The running time of the proposed method is less than that of the previous method.

***Keywords:*** *CMFD, FAST, ORB, K-means.*

*****

## 1. INTRODUCTION

Our society relies heavily on image security and authentication. It's impossible to get accurate information if an image is fabricated. In order to get accurate data, images should not be manipulated. However, these images are frequently reprinted. One of the most common methods of forgery is the copy-move forgery. The part of the region copied from the same image will be indistinguishable from the rest of the image, making it difficult for the Human Visual System to detect it (HVS). The difficulty in detecting forgery in copy move forgery detection is due to the fact that the copied blocks are from the same image, so they have the same properties as the original blocks. In other words, there are a number of ways to detect copy move forgery. Fridrich came up with the first one. They sliced an image into equal-sized blocks and arranged them in a grid. Each block's discrete cosine transformation coefficient has been extracted (DCT). Forgery detection in digital image forensics can be done in two ways. To begin, there is the "active" approach, in which digital signatures are utilized. The second approach is a passive one, and it consists of two methods. A computer-generated image or a photograph taken with a digital camera are both examples of image source identification. This method is ineffective at detecting fake images. Detection of image tampering, the second, is also available.The most common method for editing digital images is copy-move image forgery. There are many different ways to fake an image, but one of the most common methods is copy move forgery. If you use this method, the image's originality will be lost, putting its authenticity at risk. The difficulty in detecting forgery in copy move forgery detection is due to the fact that the copied blocks are from the same image, so they have the same properties as the original blocks. In the past few years, the detection of copy-move forgery has become much easier. Copy-move forgery can now be easily detected thanks to new technology and methods. Detecting copy move forgery is not an easy task. Image forgery detection using block matching techniques and Principal Component Analysis (PCA) (PCA). To detect images quickly, efficiently, and accurately through post-processing operations. Radon and the Fourier-Mellin transform are used to detect forged images [5]. Classifying textures in natural images using statistical measures and looking for discrepancies between different parts of the image

is another method for detecting forged images [6]. However, at this point, it appears that these approaches will result in a large number of missed detections and false positives. Forgery detection is difficult because blocks are extracted directly from the original image, resulting in a large number of blocks, making an exhaustive search a computationally intensive process. Forgery detection using SURF (Sped Up Robust Features) was proposed by the author, which identifies duplication regions of different sizes. [7] Detection of copy-move forgery has been proposed using a variety of methods. However, we know that the accuracy of most of these methods isn't great. To detect copy move forgery, so many of us are looking for an improved method. I'm hoping that copy move forgery detection will have a better success rate than other methods.

Forgery detection using a complex algorithm requires a lot of time and effort. It takes a long time to match each ORB descriptor with its corresponding value. So the descriptor needs to be clustered first. So, the number of counts in matching is reduced. The algorithm has become more complicated in order to save time. RANSAC, a false matching algorithm, has been used to improve the accuracy rate. When we used low-quality images, we encountered difficulties. It would be better if we used another method to improve image quality, but this would increase the difficulty of the project by a significant amount. It is possible to detect only forged images that have the same image property forgery detection method. By copying and pasting the properties of another image, this method will fail to detect a forged image.

## 2. LITERATURE REVIEW

DCT was used by Fridrich et al. [5] to extract the features of the blocks that are overlaid on top of each other. A block-based method is another name for it. In this experiment, the researchers used only a few datasets. It was the first attempt at creating a fake image. A block-based method cannot detect tempered regions if the forged region is too large.

For feature extraction, Popescu et al. [6] proposed a method based on PCA. They used a dataset of approximately 100 images of 512x512 pixels. Forged samples can't be detected using this method because it lacks responsiveness to geometric transformations, such as rotation and scaling.

According to Li [7], a block-based method is one that uses the DWT and the SVD. As long as the sample is highly compressed or edge processed, this method will work.

SIFT feature extraction was used by Huang et al. [9] and I. Amerini et al. [21] and was based on key points. An image that is too noisy or blurry cannot be identified as a forged one.

In Zhu et al. [16], ORB features help to detect the forged region of a digital image using a Scaled ORB method. Natural images from Columbia University's Natural Images Library were used to create the dataset. Time complexity is a problem because it compares all the extracted descriptors. Our proposed method outperforms the current clustering method in terms of descriptors. For this reason, it is necessary to compare the clustered centre of the forged region.

According to (AhmedTaha and Mazen M.Selim, 2021) Aya Hegazi Density-based clustering and the Guaranteed Outlier Removal algorithm are the foundations of the suggested approach. Under tough conditions, such as geometric attacks, post processing attacks, and multiple cloning, the suggested method outperforms other similar current state of the art solutions.

A new study by Navpreet Kaur Gill (2019) shows that In this case, the DCT (Discrete Cosine Transform) and SURF (Speeded Up Robust Features) features have been used to create a hybrid approach. In the face of attacks based on geometric modifications such as rotation or scaling, this strategy will demonstrate considerable results. In terms of reliability, the suggested hybrid strategy is superior to Keypoint-based methods and block-based methods, according to experimental data**.**

 ISSN: 2454-4248
30 – 41

## 3. METHODOLOGY

Scaled ORB features can be retrieved using this method.

- Image acquisition
- Identify the pyramid scale space.
- Image convert from RGB to grayscale
- Extract scaled ORB feature.
  i) Extract the FAST key points
  ii) Orientation Compute.
  iii) Build the rBRIEF feature.
- K-means++ Clustering.
- Matching feature.
- Display the forged image

### *Image Acquisition*

The first step in the detection of copy-move forgery is to take an image. Afterwards, the image should be verified and either forged or real. Lighting and camera positioning are the two most important factors affecting image quality. When taking an image for copy move forgery detection, there are a few other things to keep in mind:

**i** Image capture with adequate sharpness and resolution.
**ii** To improve recognition, images should be cleaned of any artefacts.

**Figure 3.1: Image Acquisition**

### *Image Convert from RGB to Grayscale*

An RGB image must be converted to grayscale. So that our task will be made easier by removing unnecessary data. An image can be converted to grayscale using rgb2gray. The ORB descriptor can be found in the grayscale image. This is shown in Figure 3.2

**Figure 3.2: RGB to Grayscale**

### *Identify the Pyramid Scaled Space*

It is possible to construct a pyramid scaled space using octaves and intervals thanks to David Lowe's groundbreaking work on the Gaussian pyramid [17]. The term "octave" refers to an image that has gained in resolution after being resized by a predetermined interval. Octaves can be built in intervals with help from

smoothing using Gaussian. Gaussian function, smoothing factor of Gaussian function and 'oc' octave pyramid scale space are all referred to as Loc and G(x y) respectively.

$L_{1,1}(x, y, \sigma_{1,1})$ denote the gray image of the main image I(x, y).Last pyramid scale space $L_{oc,in}$ is achieved by down sampling of the last octave by a factor 2.

$$L_{oc,in}(x, y, \sigma_{oc,in}) = G(x, y, \sigma_{oc,in}) * L_{oc,in-1}(x, y, \sigma_{oc,in-1}) \quad (3.1)$$

$$G(x, y, \sigma) = 1/2\pi\sigma^2 e^{-(x^2+y^2)/2\sigma^2} \quad (3.2)$$

In reality, this is a step in the image resizing process. Images must be divided into 2x2 sections for our convenience. The next octave of a 512x512 image will be 256x256.

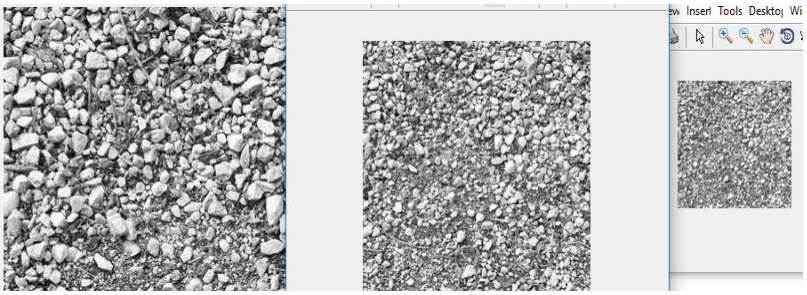


**Figure 3.3: Identify Pyramid Scale Space**

***Extract Scaled ORB Feature***

Despite the fact that the ORB feature is not a scaling-invariant descriptor, it is important in the field of image processing. Key points are assigned the pyramid scale information in order to make the feature descriptor scaling-invariant.

**i. Extract the FAST Key Points**

FAST is a fast algorithm for extracting the most important information from a large dataset. The Bresenhamcyclo-region and each pixel are the focus of this study. In order to obtain an accurate reading, we set the radius to three. To begin, determine whether the number of pixels in the Bresenhamcyclo-region surrounding the centric point(x,y) exceeds a threshold value. If it does, the centric point(x,y) is referred to as a FAST-9 point. Fast(i)=[x, y, oci, and ini] can be written as fast(i).

Built-in functions such as DetectFASTFeatures() help to identify the corners and their locations. The ORB descriptors are then extracted by applying the central moment and rotation matrix to those points. Using the following two images to demonstrate this, the first shows FAST features and the second shows ORB descriptors after applying rotation and moment.

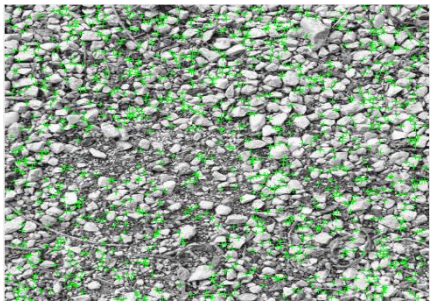


**Figure 3.4: Extract Fast Key Points**

**ii. Orientation Compute**

The moment must be taken into account when computing the orientation of those key points. Invariant moment m (p,q) is defined for the key point 'O'. First quadrant of Cartesian coordinates, where 'O' stands for origin, is where the neighbourhood N(x,y) can be easily calculated.

 ISSN: 2454-4248
30 – 41

$$m_{p,q} = \sum_{x,y} x^p y^q \, I(x,y) \quad (3.3)$$

Then, the centroid 'C' of N(x, y)is determined as

$$C=\left(\frac{m_{10}}{m_{00}}, \frac{m_{01}}{m_{00}}\right) \quad (3.4)$$

The orientation $\theta$ of the key point 'O' is determined by

$$\theta = \text{atan}\left(\frac{m_{01}}{m_{10}}\right) \quad (3.5)$$

Where, $m_{10}$ is called row moment.

$m_{01}$ is called column moment.

We get a new parameter is called Θ(Theta). So the equation becomes fast(i)=[x,y, Θ,oc,in]

***Make rBRIEF***

It is possible to steer BRIEF using the orientation of the key point, which yields the rBRIEF (Rotation-Aware BRIEF) feature with rotational invariance. A binary test's definition is based on this.

$$\tau(P:x,y) = \begin{cases} 1, & p(x) < p(y) \\ 0, & p(x) \geq p(y) \end{cases} \quad (3.6)$$

Point x is represented by p(x). The Gaussian distribution in the vicinity of point x is also satisfied by y. There are n(n=256) binary tests that make up the BRIEF feature.

$$f_n(p) = \sum_{1 \leq i \leq n} 2^{i-1} \, \tau(P:x,y) \quad (3.7)$$

A feature set of n binary tests at x and y define matrix P=$\begin{bmatrix} x1 & \dots & xn \\ y1 & \dots & yn \end{bmatrix}$. using the operation Theta(Θi) and the corresponding rotation matrix $R_\Theta$=$\begin{bmatrix} cos\Theta_i & -sin\Theta_i \\ sin\Theta_i & cos\Theta_i \end{bmatrix}$, steered matrix $P_{\Theta_i} = R\Theta_i . P$ will be constructed. Now ORB descriptor of oFAST point becomes

$$ORB(i) = f_n(p) | (x_i, y_i) \in P_\theta \quad (3.8)$$

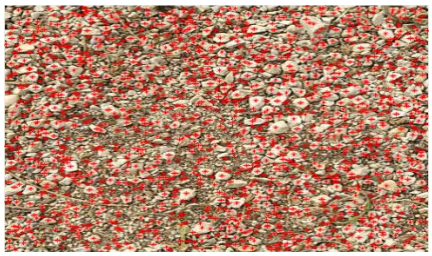


**Figure 3.5: ORB Descriptor**

***Apply K-means++***

A clustering algorithm developed by David Arthur and Sergei Vassilvitski where the centre of a K-means cluster is set as the starting point for the clustering algorithm

Calculating the distance between a data point and its nearest centre is represented by the function D(x). Following are the steps in the algorithm.

1. Pick a random centre c 1 from the list of X data points.
2. For each data point, compute D(x).
3. Weighted probabilities are used to select a new centre from the set of c i.
4. Once k centres have been chosen, repeat steps 2 and 3.
5. The standard k-means algorithm is used to finish the algorithm.

However, k-means step (5) converges very quickly after this contribution, reducing the computation time of the algorithm significantly.

 ISSN: 2454-4248
30 – 41

ORB descriptors can now be clustered with K-means++, which yields less clustered points that can be used in the matching process

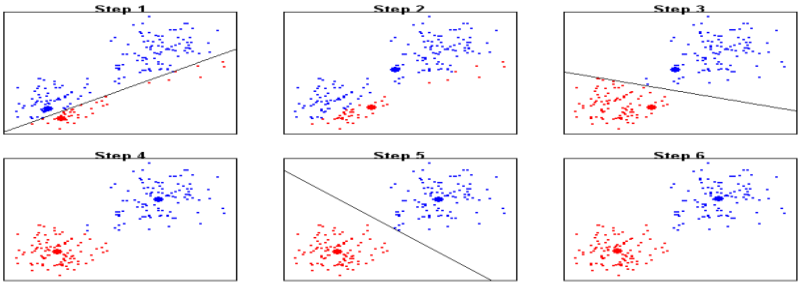



**Figure 3.6: Clustering Steps**

***Match the Feature***

Double loops are used in the feature matching process, which has a total complexity of N*N. Matching between the ORB descriptor's clusters can be done by using a double loop from 1-k.

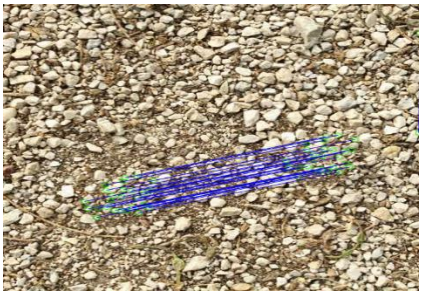


**Figure 3.7: Showing Feature Match**

***Display Image***

Now recall the main image and displaying the result with drawing the circle.

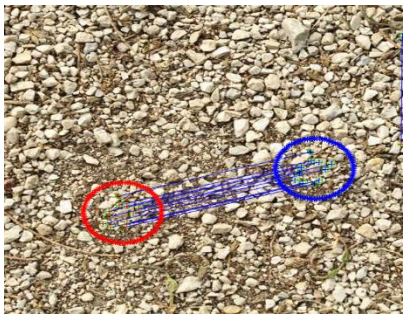


**Figure 3.8: Final Image**

## 4. RESULTS AND DISCUSSION

***Experiment Setup***

Zhu et al. [16] first used the ORB algorithm to find the ORB descriptors. Matlab R2018b and Windows 10 operating system are used in the experiment. MICC-F220 and CoMoD (small) datasets are used in this study. For testing our proposed method, we also compiled 30 datasets of various sizes.

***Results and Analysis***

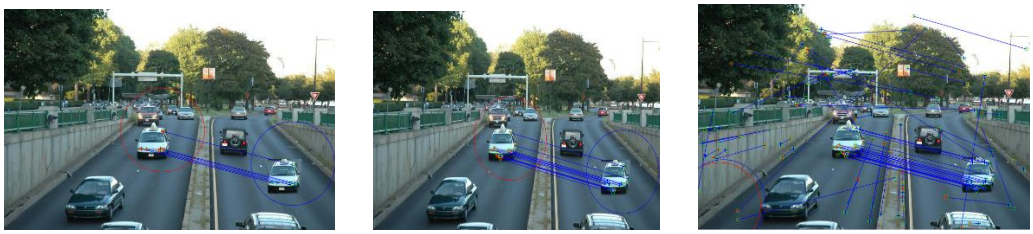
MICC-220 and CoMoFoD (small) datasets are used to test the proposed method. Some examples are 1000*700 or 700*1000 datasets that are broken up into three groups. Some non-compressed datasets have only the translation of the copied region, while others are simple scenes. PNG-formatted datasets of 512x512 pixels were released in 2013 by the CoMoFod (small) database. This dataset contains a variety of images, including translations, rotations, and scalings (40 images). Figure 4.1 (a) from the MICC-F220 dataset shows

 ISSN: 2454-4248
30 – 41

the original image. Figure 4.1 (b) depicts the cooled version of the original image (b). Figure 4.1 illustrates how the images' tempers can be detected using different threshold values. A lower threshold value results in fewer key points being uncovered. It is more difficult to extract the key points if the forged area is small in size. Consequently, it is difficult to identify the forged area. When the threshold is raised, a large number of key points are extracted, increasing the likelihood of spotting a false match.

(a) Original image (b) Tempered image

**Figure 4.1: Tempered Image with its Original Image**



(a) T=0.4 (b) T=0.5 (c) T=0.8

**Figure 4.2: Detection Result of Tampered Image in Different Threshold**

**Table 4.1**
**Matching Result with Different Threshold Value**

| **Threshold value** | 0.1 | 0.3 | 0.4 | 0.5 | 0.6 | 0.8 |
|---|---|---|---|---|---|---|
| **Number of matches** | 12 | 24 | 26 | 30 | 36 | 146 |
| **Number of false matches** | 0 | 0 | 0 | 2 | 9 | too many |

For our method to be reliable and sensitive, we used common post-processing techniques on the MICC-F220 dataset of temper images. Images from various publications and the internet were used for the most part. Threshold T=0.5 is the best value for this situation. There are fewer key points that are extracted when the threshold value is low. There are a lot of key points extracted when the threshold is high, but the probability of false matching increases significantly, as shown in the figure 4.2 (c). As a result, the threshold value is maintained at a level that is optimal for detecting forged regions. Confusion matrices are used to gauge how well the new method works. The MICC-F220 dataset, which includes 50 images, was used. Both forged and authentic images can be found in the dataset. When we ran the tests, we found that 40 forged images were detected as forged; 2 forged images were found to be forged and 3 original images were found to be original.

**Table 4.2**
**Confusion Matrics**

| **Number of images** | **TP** | **FP** | **TN** | **FP** | **Accuracy** |
|---|---|---|---|---|---|
| 50 | 40 | 5 | 2 | 3 | 86% |

 ISSN: 2454-4248
30 – 41

***Comparison with a SIFT Method***

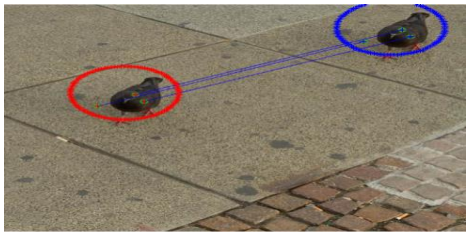
**Table 4.3**
**Comparison with SIFT Method**

| Images | Method | Elapsed time(second) | No matches of | True match | False match |
|---|---|---|---|---|---|
| 1.Baboon | ORB and K-means++ | 0.7457 | 84 | 84 | 0 |
| | SIFT | 3.8326 | 162 | 162 | 0 |
| 2.Stones | ORB and K-means++ | 1.0929 | 70 | 68 | 2 |
| | SIFT | 15.020270 | 193 | 193 | 0 |
| 3.Road and cars | ORB and K-means++ | 1.034195 | 30 | 30 | 0 |
| | SIFT | 2.5560 | 53 | 53 | 0 |
| 4.Pegion | ORB and K-means++ | 0.549761 | 46 | 46 | 0 |
| | SIFT | 2.600425 | 54 | 52 | 2 |
| 5. Grass and Number plate. | ORB and K-means++ | 0.771040 | 210 | 208 | 2 |
| | SIFT | 11.2812 | 850 | 812 | 38 |
| 6.Large coin | ORB and K-means++ | 0.621096 | 264 | 234 | 30 |
| | SIFT | 2.284661 | 366 | 292 | 74 |
| 7.Rifles | ORB and K-means++ | 0.931181 | 38 | 32 | 6 |
| | SIFT | 1.630468 | 43 | 41 | 2 |
| 8.Books | ORB and K-means++ | 0.600027 | 86 | 84 | 2 |
| | SIFT | 2.416834 | 166 | 166 | 0 |
| 9.Window | ORB and K-means++ | 0.513452 | 104 | 84 | 20 |
| | SIFT | 2.397863 | 267 | 241 | 26 |

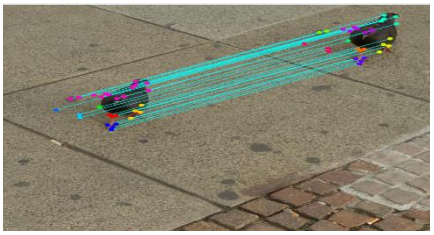
**Table 4.4**
**Matched Key Points and Running Time**

| Methods | The number of key matched points(Total) | Running time Sec (Total) | False match (Total) |
|---|---|---|---|
| SIFT (Existing Method) | 3589 | 73.3386 | 246 |
| Proposed Method | 1553 | 13.2594 | 104 |

Above table 4.4 shows the calculation of 15 forged images from the dataset of MICC-F220.

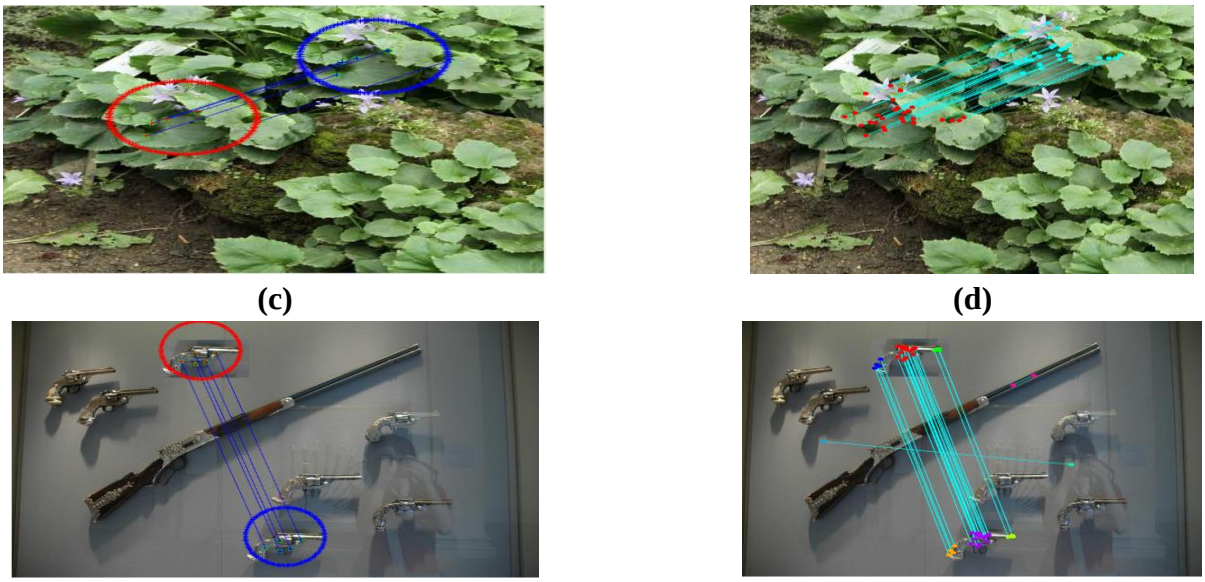


**(a)**



**(b)**

 ISSN: 2454-4248
30 – 41



**(c)** **(d)**

**(e)** **(f)**

**Figure 4.3: Result of Scaled ORB and k-means++ and SIFT Method**

**Table 4.5**
**Threshold Value Setting Based on Forged Region Detection**

| Threshold | Detection of forged region | Non forged region detected as forged |
|---|---|---|
| 0.1 | Fair | No |
| 0.3 | Fair | No |
| 0.5 | Good | No |
| 0.8 | Bad | Yes |

**Table 4.6**
**Performance Rate for Different Methods**

| Modifications | Different methods | | |
|---|---|---|---|
| | *G.Lynch[8]* | *Y.Huang[9]* | Proposed Method |
| Without Modification | 97% | 99.9% | 99.9% |
| Rotation | 0% | Only less than 5 deg. | 99.5% |
| JPEG compression | 30% | 80% | 68% |

 ISSN: 2454-4248
30 – 41

***Input Image & Output Image***

**Figure 4.4: Input Image I**

**Figure 4.5: Output image I**

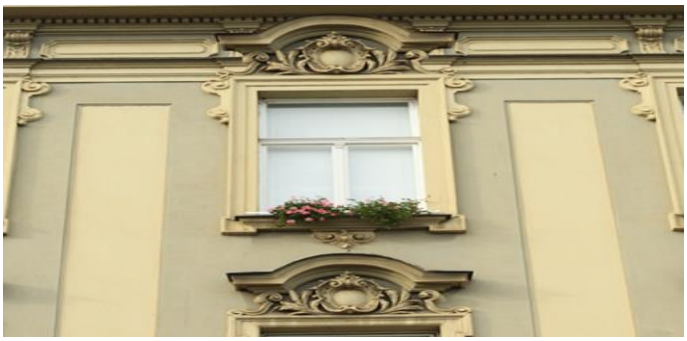


**Figure 4.6: Input image II**

**Figure 4.7: Output image II**

***Discussion***

The primary goal of this project is to develop a framework that can estimate the accuracy of the proposed algorithm by implementing it in a simulated environment. To improve copy move forgery detection, this research can be applied. We tried to establish an aesthetic framework for this project, even though the level of detection is a relative matter based on image features. The experimental results, particularly the quantitative

evaluation, show that the proposed system works well. Overall, despite some minor discrepancies in results due to environmental factors and the difficulty of manually measuring, the results can be considered satisfactory. Furthermore, it can be said that the project was successful in determining the proper level of forgery detection rate in a simulated environment.

## 5. CONCLUSION AND FUTURE WORK

### *Conclusion*

An efficient forensic method based on the scaled ORB was proposed in this work to detect the copy-move forgery of digital images. Duplicated regions are not only detected, but also the geometric transformations and post-processing applied to them. Additionally, this algorithm performs well when trying to locate duplicate regions that SIFT and SURF are unable to detect. However, high-resolution image forgery detection still takes a long time using this method.

### *Future Work*

Though our project was completed successfully, there are still areas for improvement. Image quality and accuracy would both improve with image enhancement, so let's start with that. What we think you should do next is

- Copy-paste forgery should have been flagged.
- Use a noise reduction system to improve the system's accuracy and performance.
- Try to remove any incorrect descriptors that have been flagged.
- Using a different post-processing method on the tempered image, the forged region can be identified.

Our system will be more accurate and faster when it has access to those resources. We hope to add those facilities at some point in the future, as there wasn't enough time to do so this time around. In addition, our system was superior to previous systems in many ways. For copy move forgery detection, I'm hoping one of these systems will be the best.

## REFERENCES

[1] Mahdian, Babak, and S. Saic. “Detection of copy-move forgery using a method based on blur moment invariants”, *Forensic science international* 171.2 (2007): 180-189.

[2] Huang, Hailing, W.Guo, and Y. Zhang. “Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm”, *Computational Intelligence and Industrial Application*, 2008. PACIIA’08. Pacifc-Asia Workshop on. Vol. 2. IEEE,2008.

[3] M. Fischler, Bolles, “Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography ”, *Communications of the ACM 24, 6(1981),381-395*

[4] Qureshi, M. Ali, and M. Deriche “A bibliography of pixel-based blind image forgery detection techniques”, *Signal Processing: Image Communication 39* (2015): 46-74.

[5] Fridrich., Soukal, and Lukas, A.J., “Detection of Copy-Move Forgery in Digital Images”, *In Proceedings of Digital Forensic Research Workshop, Citeseer(2003)*.

[6] Popescu, Farid, “Exposing digital forgeries by detecting duplicated image regions*”, Dept. Comput.Sci., Darmouth College, Tech. Rep*. TR2004-515,(2004).

[7] Li, Guohui, et al. “A sorted neighbourhood approach for detecting duplicate regions in image forgeries based on DWT and SVD”, *Multimedia and Expo, 2007 IEEE International Conference on. IEEE,2007.*

[8] Gavin Lynch, Frank Y. Shih, Hong-Yuan Mark Liao,An efficient expanding block algorithm for image copy-move forgery detection,Information Sciences, Volume 239, 2013, Pages 253-265, ISSN 0020-0255,https://doi.org/10.1016/j.ins.2013.03.028.

[9] Huang, Yanping, et al. “Improved DCT-based detection of copy-move forgery in images”, *Forensic science international* 206.1 (2011):178-184.

[10] B.Yang, X. Sun, H. Guo, Z. Xia, X. Chen. “A copy move forgery detection method based of CMFD-SIFT”.

[11] Pan, Xunyu, and S. Lyu. "Region duplication detection using image feature matching", *Information Forensic and Security*, IEEE Transactions on 5.4(2010): 857-867.

[12] Jaberi, Maryam et al. "Accurate and roboust localization of duplicated region in copy-move image forgery", *Machine vision and applications* 25.2.(2014):451-475

[13] Shivakumar, and L. D. S. S. Baboo. "Detection of Region Duplication Forgery in Digital Images Using SURF", *IJCSI International Journal of Computer Science Issue* 8.4(2011).

[14] Bo, Xu, et al. "Image Copy-Move Forgery Detection Based on SURF", *Multimedia Information Networking and Security (MINES),2010 International Conference on IEEE,* 2010.

[15] Isaac, M. Mary, and M. Wilscy. "Copy-Move forgery detection based on Harris Corner points and BRISK", *Proceedings of the Third Internation Symposium on Women in Computing and Informatics.* ACM,2015.

[16] Zhu, Ye, X. Shen, and H. Chen. "Copy-move forgery detection based on scaled ORB", *Multimedia Tools and Applications(2015*): 1-13.

[17] D Arthur, S. vassilvitskii, "K-means++ : the advantages of careful seeding", *in Proceedings of the 18th SODA,2007*,pp,1027-1035.

[18] M. Fischler, Bolles "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography", Commun ACM 24:381-395.

[19] Amerini, Irene, et al. "A sift-based forensic method for copy-move attack detection and transformation recovery", *Information Forensics and Security, IEEE Transactions on 6.3 (*2011): 1099-1110.

[20] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme", *IEEE Trans. Inform. Forensics and Security,* vol. 10, no. 3, pp.507-518, March 2015.

[21] P. Kakar and N. Sudha, "Exposing postprocessed copypaste forgeries through transform-invariant features", *IEEE Trans. Inf. Forensics Security, vol. 7, no. 3,* pp. 10181028, jun.2012.

[22] Wen Zhang, Jie Men, Conglong Ma, "Research progress of applying digital watermarking technology for printing," 2018, IEEE

[23] David-Octavio Muñoz-Ramirez, Volodymyr Ponomaryo, Rogelio Reyes-Reyes, Volodymyr Kyrychenko, Oleksandr Pechenin, Alexander Totsky, "A Robust Watermarking Scheme to JPEG Compression for Embedding a Color Watermark into Digital Images," 2018, IEEE

[24] AnirbanPatra*, Arijit Saha, Ajoy Kumar Chakraborty, Kallol Bhattacharya, "A New Approach to Invisible Water Marking of Color Images using Alpha Blending," 2018, IEEE

[25] Irshad Ahmad Ansari, Chang Wook Ahn and Millie Pant, "On the Security of "Block-based SVD image watermarking in spatial and transform domains", 2018, IEEE

[26] Alexander S. Komarov, "Adaptive Probability Thresholding in Automated Ice and Open Water Detection From RADARSAT-2 Images," 2018, IEEE

[27] Aoshuang Dong, Rui Zeng, "Research and Implementation Based on Three-dimensional Model Watermarking Algorithm," 2017, IEEE

[28] Enjian Bai, Yiyu Yang and Xueqin Jiang, "Image Digital Watermarking Based on a Novel Clock-controlled Generator," 2017, IEEE

[29] Oleg Evsutin, Roman Meshcheryakov, Viktor Genrikh, Denis Nekrasov and Nikolai Yugov, "An Improved Algorithm of Digital Watermarking Based on Wavelet Transform Using Learning Automata," 2017, IEEE

[30] Ritu Gill and Rishi Soni, "Digital Image Watermarking using 2-DCT and 2- DWT in Gray Images," 2017, IEEE.

[31] Mohammad Shahab Goli and Alireza Naghsh, "Introducing a New Method Robust Against Crop Attack In Digital Image Watermarking Using Two-Step Sudoku," 2017, IEEE

[32] Muhammad Usman, Irfan Ahmed, Shujaat khan, "SIT: A lightweight encryption algorithm for secure internet of things," international journal of advanced computer science and applications, vol. 8, no.1, 2017.

[33] Aya Hegazi, Ahmed Taha, Mazen M. Selim,An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal,Journal of King Saud University - Computer and Information Sciences,Volume 33, Issue 9,2021,Pages 1055-1063,ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2019.07.007.

[34] Navpreet Kaur Gill, 2019, An Efficient Approach for Detection of Digital Photo Forgery using Copy-Cover Techniques, International Journal Of Engineering Research & Technology (IJERT) Volume 08, Issue 11 (November 2019).

[35] Chengyou Wang , Zhi Zhang , Qianwen Li , And Xiao Zhou, An Image Copy-Move Forgery Detection Method Based on SURF and PCET, 2019, IEEE.