Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7760109

DETECTION OF COPY MOVE FORGERY USING ROOTSIFT AND FEATURE POINT MATCHING

Litty Koshy
Research Scholar,Department of CSE, Sathyabama Institute of Science and Technology,
Chennai, India, grace.koshy@gmail.com

Prayla Shyry S
Professor, Department of School of Computing,Sathyabama Institute of Science and
Technology, Chennai, India, praylashyry@sathaybama.ac.in

Abstract

The popularity of the internet has grown recently, making it simpler to broadcast and purchase digital content. This popularity suggests that counterfeiting has increased the susceptibility of multimedia to modification. A copy-move forgery is one of the most popular techniques for digital photo modification. Key point-based detection systems have successfully exposed copy-move forgery as a result of various digital assaults. On the other hand, these methods are useless when forgeries only involve tiny, smooth areas with a small number of crucial spots. A multi-scale feature matching based on the copy-move forgery detection technique was put into place to solve these problems. I believe the copy move method has some potential as well. Reduce the intensity threshold and rescale the supplied image to produce a reasonable number of key points in order to address those concerns in the proposed system initially. Then, a special multi-scale matching method is developed using scale clustering, overlapping grey scale clustering, and group matching modules. Present a novel iterative localization strategy that locates the forged region by utilising the resilience properties of each key points as well as its colour information. According to the experimental results, the suggested work's copy move forgery average is 1.375, compared to the existing system's average of 2.75, with standard deviations of 0.72 and 1.44, respectively. As a result, we can say that the proposed approach is more accurate and efficient than existing methods by more than 99.9%.

Keywords: Multi-scale feature matching, Scale clustering, Keypoint, Iterative localization, Copy-Move forgery

1. Introduction

The digital revolution is transforming the way we exchange and manipulate data, but it has also created a slew of serious security vulnerabilities that threaten the integrity of digital material [7]. Image manipulation has become a common technique because of advanced digital technologies and photo-editing tools like Adobe Photoshop. As a result, digital photographs are becoming more vulnerable to forgery, eroding their credibility of digital images. Individuals (false photographs of celebrities and prominent personalities), society (fake images targeting religion or ethnicity), and media are all victims of digital forgeries. According to a poll, Flickr has 350 million photos, with over 1 million added every day (record 2007), while Facebook has over 50 million cumulative picture submissions (as the record in 2010). The preservation of such vast amounts of digital data has become crucial, complicated, and difficult. Digital Images Forensics (DIF) is a cutting-edge security approach that aims to restore lost confidence in digital photos by uncovering digital forgery tactics.

The goal of this study is to create a fast and efficient key point-based technique for detecting and localizing copy-move forgeries that usually makes good results even when the forgery only includes tiny and smooth areas, or the forged images are subjected to several serious attacks. Different steps, involved in this process are Extraction of features, Matching of features, and finally localizing the forgery. Designing unique and complex solutions for all three processes is the key contribution. In the first stage, RootSIFT, a SIFT[4](Scale Invariant Feature Transform) modification, develop a strategy for extracting a sufficient number of key points from tiny and smooth areas. In order to handle keypoint matching concerns with a large number of key points, a special feature point matching technique [6] is recommended in the second stage.

The third stage then proposes methodologies for estimate of homography and localisation that do not require any clustering or segmentation techniques. The technique produces extremely accurate identification results at a much-reduced computing cost by fully leveraging the resilience features such as scale value, orientation, and each key point's RGB value.

2. Related work

The techniques for detecting picture forgeries come in two flavours: Active Approach and Passive (blind) Approach[5]. In active approaches, pre-registration or pre-embedded information is used. To protect the photos from being modified, a shield is created, mostly based on digital watermarking. The fundamental downside of this strategy is that it requires anti-manipulation measures. This drawback is solved by adopting a passive technique, which may also cater to pre-existing pictures. These methods are built on the idea that, while multimedia forgery may leave no visible signs of manipulation, they might change an image's underlying data. Digital photo forgeries can be made easily and successfully using the technique of "region duplication"[1], which involves copying and pasting a continuous section of pixels from one image to another while potentially changing its geometry and lighting. The currently existing methods for detecting region duplication rely on block matching of pixels or transform coefficients, which is ineffective when the repeated regions have anomalous geometry or lighting. This work presents a duplicated region-insensitive area repetition detection technique.

After discarding the calculated transforms, the approach discovers all pixels within the duplicated areas by estimating the transform between matching key points, which are impervious to geometrical and lighting aberrations. On an autonomously generated forgery picture database containing duplicated and warped parts, the suggested approach successfully detects forgeries. The authors of [2] and [8] discussed a method for precisely identifying and localizing copy-move forgeries that is based on rotation-invariant properties generated densely on the image. Dense-field approaches suggested in the literature provide improved performance than key point-based equivalents at the expense of significantly longer computation, owing to the feature matching step. Patch-Match, an NN search designed specifically for the calculation of dense fields over pictures, is presented to address this constraint. In order to deal with invariant properties efficiently, a matching method is changed. As a result, the method is more resistant to rotations and scale changes. Furthermore, based on the smoothness of the output field, a simpler and more dependable post-processing method is developed. According to experimental studies on online datasets, the recommended appears to be more accurate and durable. The difficulty of identifying if a picture has been forged is studied, according to the authors in [3], with special emphasis devoted to the instance in which one section of an image is duplicated and then affixed into another area to make a duplication or to remove anything problematic. In most cases, a geometric adjustment is required for adapting the picture patch to the new environment. A unique SIFT-based algorithm is presented to detect such changes[28]-[30]. This approach enables us to determine whether an attack has happened as well as retrieve the geometric transformation utilized for cloning. The technique can effectively identify the transformed region and estimate the geometric transformation parameters with high accuracy, according to a large body of experimental data. This approach also addresses multiple cloning. The main goal of the author's research is to improve the detection of cloned picture patches with very uniform texture and obvious critical points that cannot be retrieved by SIFT-like methods. In[9], an example of PRNU, localization of forgery based on photo-response non-uniformity noise was presented, which proposes a segmentation-based forgery localization scheme that takes advantage of the local given, which suggests a segmentation-based forgery localization method to get around the drawbacks of current segmentation algorithms that are simply focused on perceivable content. This method makes use of the local homogeneity of obviously unidentifiable information. The authors provided a multi-orientation localization method that combines multi-oriented detection windows and the forgery probability learned by image segmentation. In the case of hard-boundary forgeries, this technique helps boost forgery localization efficiency based on imperceptible forensic evidence, but segmentation based only on visual content has the potential to be ineffectual in the case of soft-boundary forgeries. Homogeneity of clearly unidentifiable clues to overcome the limitations of existing segmentation approaches that are solely based on perceivable content [32]. The authors offered a multi-orientation localization approach that combines the forgery probability acquired by picture segmentation with multi-oriented detection windows. This method helps increase forgery localization efficiency based on undetectable forensic indications, particularly for hard-boundary forgeries, while segmentation based only on visual content has the potential to be ineffective, in the case of soft-boundary forgeries.

The primary disadvantages of existing key point copy-move forgery detection systems are:

a) They fail to create a significant number of key points, which involve tiny or smooth copy move areas. That is, resulting in detection failure for soft-boundary forgeries.

b) It is exceedingly difficult to develop a segmentation method and associated parameters that are widely recognized and effective for all photos. This is so that the copy-move sections can have a wide range of textures and sizes. The amount of copy-move areas is typically unknown as well, which makes the clustering procedure difficult in this circumstance..

The robustness of the block features against some common distortions, like geometric changes, has been improved using the discrete cosine transform (DCT) [10], discrete wavelet transform (DWT) [11], principal component analysis (PCA) [12], singular value decomposition (SVD) [13], and other techniques [14],[15]. [17] advocated that adaptive Matching be used to discover duplicated regions within the same picture and that an adjustable threshold be utilized in the matching phase to eliminate false matches. This strategy can reduce the number of incorrect matches by a substantial amount, resulting in increased performance and decreased computation costs. But accuracy, on the other hand, is an issue. D An technique based on WT-DCT[18] for detecting copy move fraud. To identify forgeries, the authors developed a new method based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform Quantization Coefficients Decomposition (DCT-QCD). After using DWT to partition the image, the author used DCT-QCD to minimize the row vectors (Quantization coefficient decomposition). The shift vector is calculated after sorting, then compared to the threshold, and lastly, the tampered portion of the picture is highlighted. Nowadays to make the final forgeries more realistic, the attacks can also be combined with techniques to rotate, scale, compress, and add noise Detecting them can be difficult, particularly when forgery using copy-move techniques only affects tiny or smooth sections, or when the faked portions have been subjected to grim attacks like massive scaling and excessive addition of noise. A unique algorithm based on Root SIFT is suggested to detect such alterations. This approach enables us to determine whether a copy-move attack has happened as well as retrieve the geometric transformation utilized for cloning. To illustrate that the method can accurately identify the converted region and estimate the geometric transformation parameters, experimental data is shown. A copy-move forgery is created by cutting off portions of one image, pasting them into another, and sometimes post-processing it. The detection of copy-move forgeries has been one of the most thoroughly researched subjects in picture forensics in recent years. Numerous unique algorithms focusing on various post-processed copies have been presented. The major goal of this study is to identify the forgery detection algorithms and post-processing methods that perform best under various post-processing conditions. The investigation's goal is to evaluate the performance of feature sets that have previously been offered. This could be done by integrating numerous algorithms into a single pipeline. The suggested method completely utilizes the resiliency features of each key point, including its dominant orientation and size information, to deliver exceptionally accurate identification results at a significantly reduced computing cost. In this study, the top 15 feature sets are investigated. On a per-pixel and per-image basis, the detection performance is assessed. Keypoint-based features SURF, ORB, SIFT, and PCA fared exceptionally well in experiments. The detailed study of the related works are given in the following table 1

Table 1 : Literature Review

S.No	Name of the Researcher	Title of the Research	Concept	Disadvantage
1	Amerin and all.	Geometric tampering estimation using a forensic investigation based on SIFT	This technique, which is based on SIFT features, enables the recovery of the geometric transformation's parameters as well as the identification of the image points implicated in the counterfeit attack.[19]	There is no discussion of how the approach behaves in relation to the size and texture of the cloned image patch.
2	S. Lyu and H. Farid	The degree of photorealism	A technique is used to distinguish between photographic and photorealistic images.[20]	The disadvantage of this, in terms of rendering, is that these models may not always provide any guidance on how one may produce images that are more lifelike.

3	H. Farid	detection of fake images	Discussed detailed study of image forgery detection.[21]	Copy move problem is not identified
4	Zhigang Fan and R. L. de Queiroz	History of bitmap compression identification: quantizer estimation and JPEG detection.	created a technique for estimating JPEG quantization steps with the highest degree of certainty.[22]	It only displayed the results for black and white pictures. The next logical step in this continuing research project is to use colour photographs.
5	Cozzolino, Davide, and all	Using patchmatch, copy-move forgery detection is detected.	It uses PatchMatch, an iterative randomised nearest-neighbor search technique that takes advantage of natural images' regularity to quickly conver to a nearly ideal and smooth field.[23]	It is much slower than the other techniques.
6	Bi, Xiuli and all	Utilizing local bidirectional coherency error refinement, quickly detect copy-move forgeries	In order to determine the feature correspondences in an image, it first adapts and improves a coherency sensitive hashing approach.[24]	The feature correspondences are then improved via an iterative process over the enhanced coherency sensitive search using a local bidirectional coherency error.
7	Shabanian, Hanieh and all	An innovative method for spotting copy-move fraud in digital photographs	As a method for similarity matching, it employs the structural similarity index. Additionally, we are able to significantly increase the approach's run-time speed thanks to the Gaussian pyramid decomposition method.[25]	It is only supported for post processing oprations.
8	Wang, Xiang-Yang, et al	For tiny smooth regions, a new keypoint-based copy-move forgery detection method	It is founded on the quaternion polar complex exponential transform and the colour invariance paradigm (QPCET).[26]	No clear local visual cues are provided for accurately defining the content of the Delaunay triangle.
9	Aloraini, Mohammed, et al	For the detection and localization of object removal video forgeries, sequential and patch analyses	To locate forged portions in films and identify object removal forgery, sequential and patch analysis are used.[27]	The use of asymptotic local hypotheses in non-additive change models, such as variations in covariance or correlations, is not entirely evident.
10	Pandey,et and all	detection of passive copy-move forgery in videos	Forensic techniques that are passive have been thought of for CMFD in the spatial and temporal domain of video. Scale Invariant Features Transform (SIFT) is presented for detecting copy-move fraud in the spatial domain.[31]	Detecting video splicing in extremely compressed video is still difficult to do.

3. Proposed System

The proposed system is put into place to fix the issues with the current systems. The image that would be used to communicate between users was taken as an input at first. The following processes, which are illustrated in the following figure.1, are used to process that image with the aid of the root sifting and feature point matching algorithms.

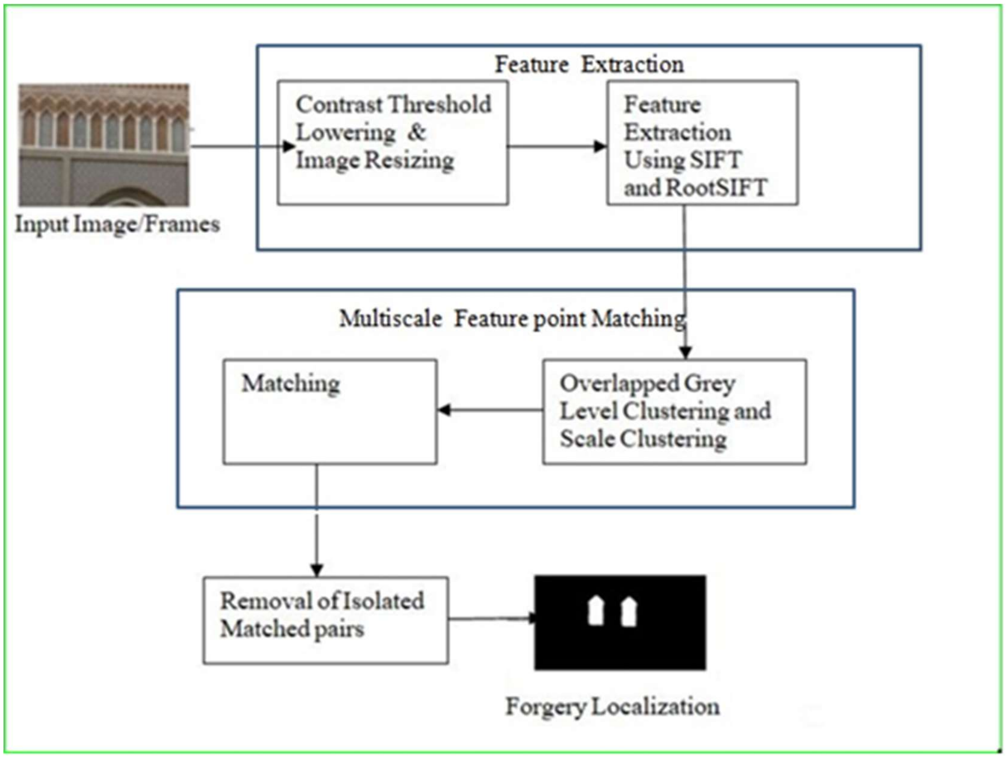

Feature Extraction
Contrast Threshold Lowering & Image Resizing
Feature Extraction Using SIFT and RootSIFT
Input Image/Frames
Multiscale Feature point Matching
Matching
Overlapped Grey Level Clustering and Scale Clustering
Removal of Isolated Matched pairs
Forgery Localization

Figure 1. System Architecture

A) Feature Extraction

Reducing the contrast threshold and resizing the input image are two straightforward but effective ways to extract a significant number of critical points from the first step of feature extraction, even from smooth and minute regions. A threshold is used for the rejection of unstable extrema having low contrast values. The challenge of creating a sufficient number of key points cannot be solved by decreasing the contrast threshold alone. When copy-move forgery is carried out on tiny areas. The supplied image is resized by a factor of two as a complementary technique. The proposed system generates key points based on SIFT and ROOFSIFT. The SIFT technique is separated into four phases:

- Identifying Candidate key points.
- Refining of key points based on contrast and edge thresholds.
- Each key point’s dominant orientation assignment
- Generation of feature descriptor

At the start of phase 1, candidate Key points are selected on various scales. Consecutive Gaussian-blurred photos are formed from an input image I by repeatedly convolving it using Gaussian filters at various sizes. Then, local extrema inside a 3 x 3 x 3 Difference of Gaussians (DoG) zone are selected as the prospective critical spots. All potential crucial locations are further adjusted in phase 2 using a contrast and edge threshold. The SIFT algorithm's removal of unstable extrema depends on this strategy. Phase 3 involves assigning a dominant orientation to each important point that survives in order to guarantee rotation invariance. Aggregating gradient orientation information, a histogram for orientation is produced from points in a local window centered on the SIFT key point. In step 4, a 128-dimensional descriptor is produced by coding the surrounding information in a restricted area using the SIFT key point. Simply lowering the contrast threshold won't solve the issue of getting enough key points when copy-move forgery is used on tiny areas. Before computing SIFT key points, enlarge the input picture by a factor of S. Then comparing histograms, the Hellinger kernel or the chi-squared distance generally outperforms the Euclidean distance. Most of the SIFT articles describe comparing descriptors using the Euclidean distance, SIFT is still a histogram itself. As a result, rather than employing a separate measure to compare SIFT descriptors, the 128-dim descriptor produced by SIFT can be adjusted. RootSIFT, proposed by Arandjelovic et al[4], is a simple algebraic modification to the SIFT descriptor that allows SIFT descriptors to be "compared" using a Hellinger kernel. The following is a basic approach for extending SIFT to RootSIFT:

Feature Extraction Algorithm :

Input : Image / Frame

```
Output resized and feature extracted image
Step 1: initialize the SIFT feature extractor and then Compute SIFT descriptors.
Step 2: if there are no key points or descriptors, return an empty tuple.
Step 3: Apply the Hellinger kernel by first L1-normalizing and taking the square root.
Step 4: Then the vectors are L2-normalized and return a tuple of the key points and descriptors.
```

B) Matching of Feature Points

The matching of feature points in the copy-move forgery detection scenario searches the picture for comparable local areas. Scale clustering is a matching technique that calculates the distance between each key point in a cluster to identify the keypoint k's matched correspondence (C1, C2, or C3). The more crucial sites there were, the greater the computing overhead would be. An effective matching approach is even more crucial in this design since the feature extraction process generates a high number of key points. To hasten the matching procedure, a method known as overlapping grey level clustering is applied. The suggested method can be used to carry out the matching procedure much more effectively without having to eliminate initial valid matches. The key points are divided into clusters that overlap. The nearby clusters, in particular, will share a portion of the key points. Initially, based on the RGB values [0, 1, ….., 255] is evenly split into M intersecting sub-levels, each having a length of c1 and an intersecting length of c2. It's important to note that none of the matched pairs in P are in any particular order. Because the matching procedure ignores the location information, it is unable to provide a constant matching direction.

C) Localization of Forged Region

Localization identifies duplicated spots in sparse fields in the forgery detection scenario. When it comes to locating the fraudulent portions, keypoint-based picture copy-move forgery detection[29] approaches have two problems. 2) Because there is typically no matching order in matched pairs, the forged points and their original counterparts are not broken up during the matching process, even when many clones are made, the homography is typically distinct and the percentage of duplicated areas is unknown. The framework of the suggested forgery localization approach is made up of four parts.

Step 1) First, isolated matched pairings are eliminated or each matched pair is removed to lower the false alarm rate. (m, m') Є P, where P is defined as the set containing all matched pairs, let Nm and Nm' be the numbers of matching points with location distances to m and m' lesser than some threshold T.Here matched pairs that satisfying Eq(1) is discarded.

$$\max\{ N_m , N_{m'} \} < N_T \quad (1)$$

After this step, M is a new set consisting of the matched survived pairs.

Step 2): For homographic estimation, a subset of related pairs from two nearby local areas will be used to estimate an affine matrix. After selecting a matched pair at random, all matched key points around the selected matched pair are recorded. All the related pairs that are near to the given matched pairs are combined to form a new set. It's worth noting that all of the related pairs in the set have the same matching order. Because all of the related pairings in the collection are made up of two contiguous local areas, it's safe to conclude that they all follow the same homography. The homography between correspondence of the matched pairs in the set is estimated using the RANSAC algorithm [16].

Step 3): Validation of homography and selection of inliers based on prevailing orientation. To discard inaccurate estimation from RANSAC, by accentuating the prevailing orientation associated with each keypoint, a homography validation, and inlier selection strategy has been developed. The offset of the dominating orientations for each inlier must be consistent with the predicted affine homography. Correctness of the estimated homography is validated by a function f defined as :

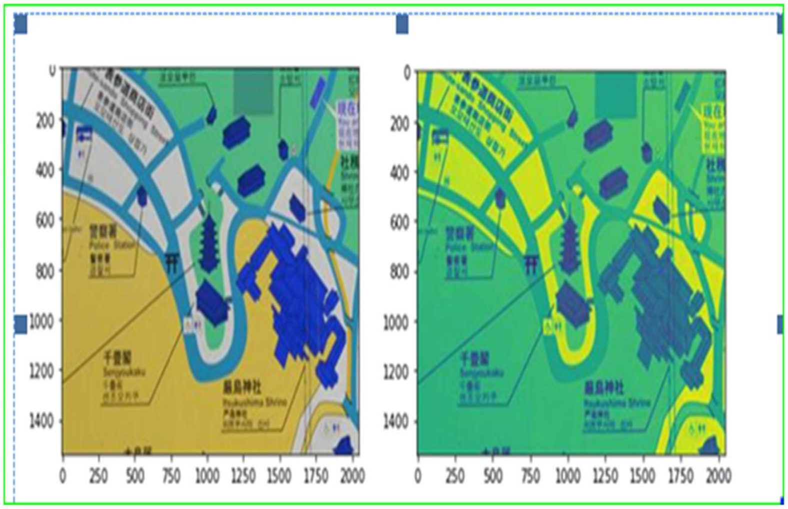
$$f(m, m', H_{m)} = | \theta_{m'} - \theta_m - \theta_H | \quad (2)$$

For an adequately computed homography and correctly matched pair, the function f is near zero. To avoid the occurrence of inliers that are incorrectly accepted by chance, we accept the homography if and only if the new set matches over 90% of the time.

Step 4): Localization of forgery using the scale and RGB information. There are two phases to this approach i.e i) construction of suspicious regions and (ii) refinement of suspicious regions. A local suspected region is created in the first step based on the scale information of each inlier. In the second phase, the suspicious regions are refined by exploiting the color information. This localization algorithm operates iteratively and will be repeated for N iterations. After finishing all the iterations, the detected forgery regions can be generated.

4. Experiment and Result Analysis

The dataset used is the GRIP dataset. This GRIP dataset includes 80 genuine photos and 80 realistic copy-move forgeries, all of which are 768 x 1024 pixels in size. It's worth noting that certain manipulated patches in GRIP are highly smooth, which makes copy-move forgery detectors based on sparse sampling difficult to detect.



(a) (b)

Figure 2.(a) Input Image (b) Output Image

Figure 2 (a) is fed into the algorithm as input. It is converted into a grey image which is shown in Figure 2(b). Then the grey image is fed into the RootSIFT algorithm and the key points are extracted as shown in Figure 3. The red dots depict RootSIFT key points.

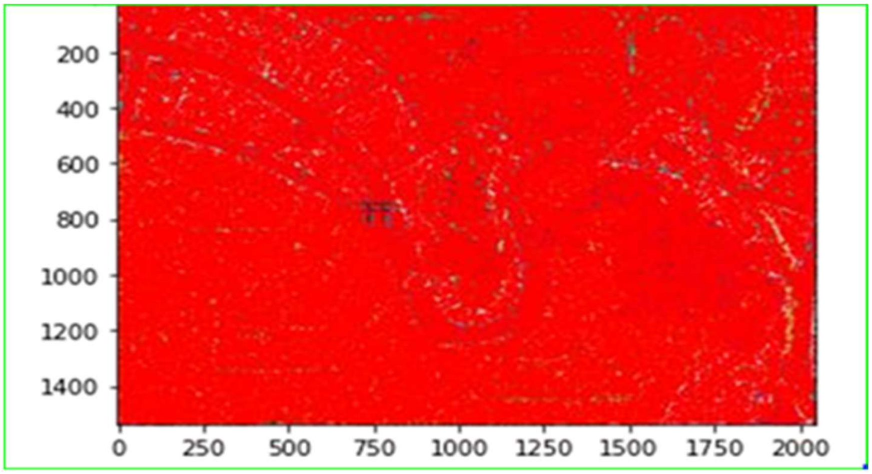
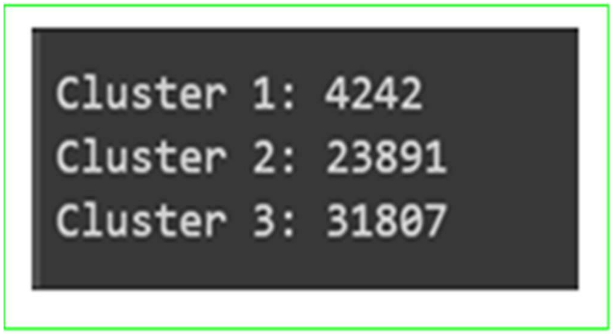


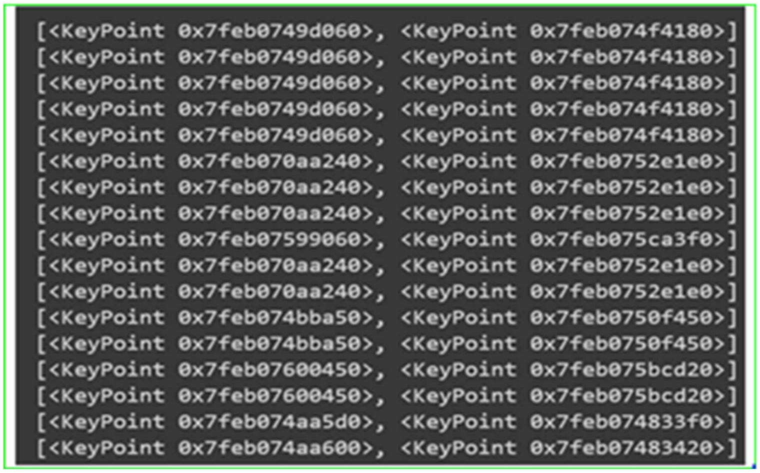
Figure 3. RootSIFT Keypoints



```
Cluster 1: 4242
Cluster 2: 23891
Cluster 3: 31807
```

Figure 4 . Scale Clustering

Three categories of key points have been identified based on their scale values. The number of key points in each cluster is shown in Figure 4. Then after overlapped grey level clustering, a matching procedure is conducted. Some of the matched pairs of cluster1 are in Figure 5.



```
[<KeyPoint 0x7feb0749d060>, <KeyPoint 0x7feb074f4180>]
[<KeyPoint 0x7feb0749d060>, <KeyPoint 0x7feb074f4180>]
[<KeyPoint 0x7feb0749d060>, <KeyPoint 0x7feb074f4180>]
[<KeyPoint 0x7feb0749d060>, <KeyPoint 0x7feb074f4180>]
[<KeyPoint 0x7feb0749d060>, <KeyPoint 0x7feb074f4180>]
[<KeyPoint 0x7feb070aa240>, <KeyPoint 0x7feb0752e1e0>]
[<KeyPoint 0x7feb070aa240>, <KeyPoint 0x7feb0752e1e0>]
[<KeyPoint 0x7feb070aa240>, <KeyPoint 0x7feb0752e1e0>]
[<KeyPoint 0x7feb07599060>, <KeyPoint 0x7feb075ca3f0>]
[<KeyPoint 0x7feb070aa240>, <KeyPoint 0x7feb0752e1e0>]
[<KeyPoint 0x7feb070aa240>, <KeyPoint 0x7feb0752e1e0>]
[<KeyPoint 0x7feb074bba50>, <KeyPoint 0x7feb0750f450>]
[<KeyPoint 0x7feb074bba50>, <KeyPoint 0x7feb0750f450>]
[<KeyPoint 0x7feb07600450>, <KeyPoint 0x7feb075bcd20>]
[<KeyPoint 0x7feb07600450>, <KeyPoint 0x7feb075bcd20>]
[<KeyPoint 0x7feb074aa5d0>, <KeyPoint 0x7feb074833f0>]
[<KeyPoint 0x7feb074aa600>, <KeyPoint 0x7feb07483420>]
```

Figure 5:Matched Pairs.

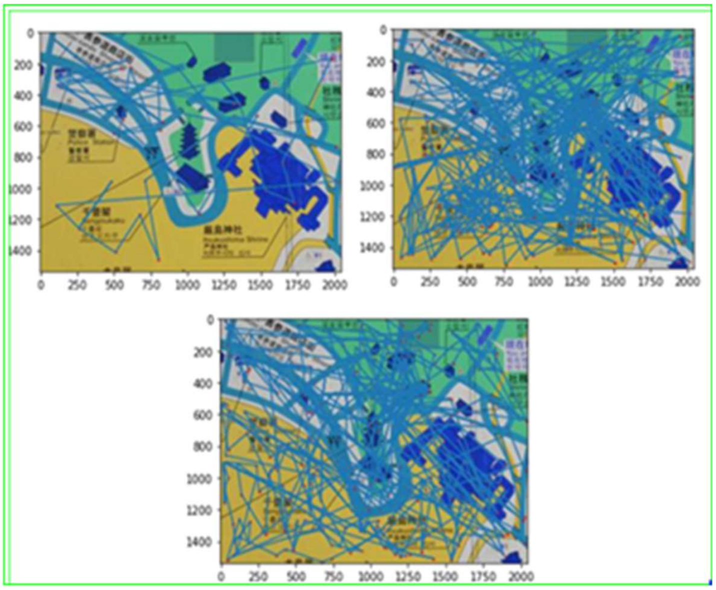
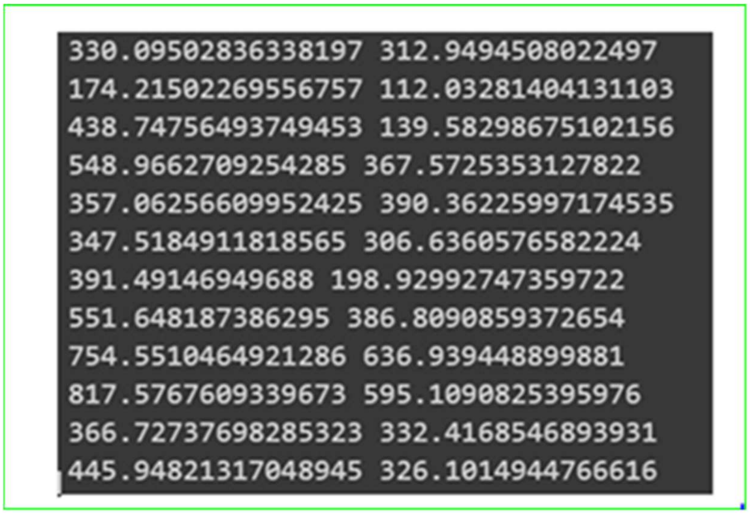


Figure 6: Matched Pairs for three Clusters

Figure 6 plots the matched pairs of each cluster on the image. The blue lines joining the red dots indicate the matched pairs. In phase 3, the isolated matched pairs are detected based on a certain threshold. Some of the isolated matched pairs are shown in Figure 7. These matched pairs are to be removed from the set of detected matched pairs.



```
330.09502836338197 312.9494508022497
174.21502269556757 112.03281404131103
438.74756493749453 139.58298675102156
548.9662709254285 367.5725353127822
357.06256609952425 390.36225997174535
347.5184911818565 306.6360576582224
391.49146949688 198.92992747359722
551.648187386295 386.8090859372654
754.5510464921286 636.939448899881
817.5767609339673 595.1090825395976
366.72737698285323 332.4168546893931
445.94821317048945 326.1014944766616
```

Figure 7:Isolated Matched Pairs

The final output obtained after executing the iterative forgery localization algorithm is shown in Figure 8.

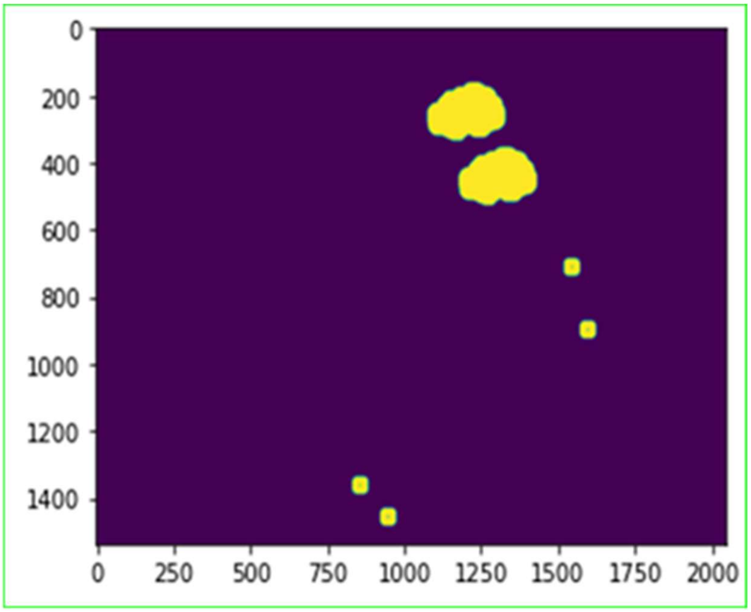


Figure 8: Final output

Figure 9 depicts the performance evaluation between SIFT and RootSIFT in terms of accuracy. The graph is plotted according to the values obtained from four different images. The graph shows an accuracy of 99% if ROOTSIFT is used for the image forgery analysis whereas SIFT provides an accuracy of 98%.

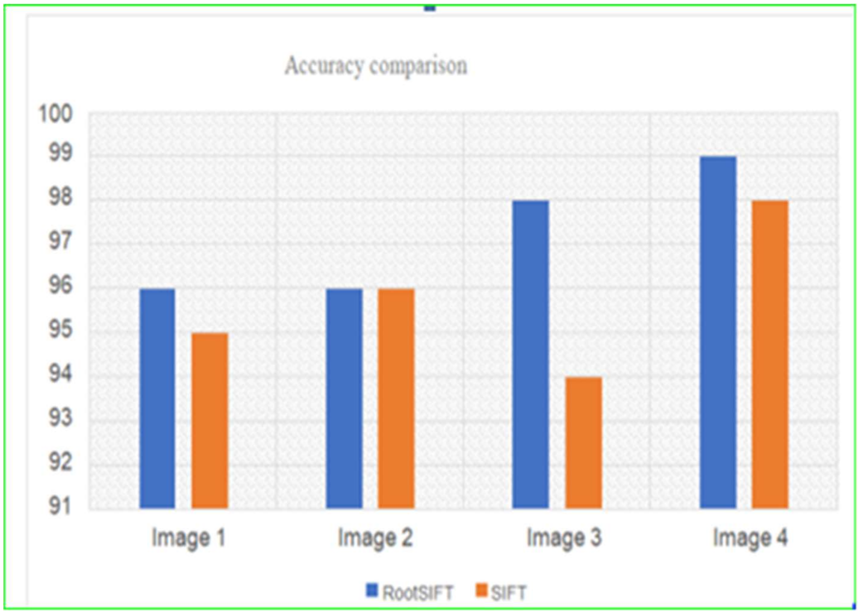


Figure 9. Performance Evaluation Graph

It is most frequently used when the test statistic would have a normal distribution if the test statistic's scaling term's value were known. When the scaling term is unknown and is replaced with an approximation based on the data, the test statistic (under certain circumstances) follows a Student's t distribution.

$$\bar{x}_1 = \sum \frac{x_1}{n} = 1.375$$

$$\bar{x}_2 = \sum \frac{x_2}{n} = 2.75$$

According to the results of the previous analysis, the mean values of the suggested work and the SIFT process are respectively 1.375 and 2.75, with standard deviations of 0.72 and 1.44. There are statistically significant differences in both cases, as evidenced by the two-tailed P value of 0.0193, which is less than 0.05. Second, compared to SIFT, the mean value of the proposed systems (1.375) is significantly lower (2.75). It can be seen that the proposed framework's copy and move forgery risks are much lower and appear to be better when compared to the suggested system's copy and move forgery potentials and those of the current system.

5. Conclusion

In the real world, all communications particularly those between forensics departments, government agencies, and other entities require the sharing of data without any copying, moving, or duplicate labor. The key point-based copy-move forgery detection and localization technique are the main topics of this suggested work. It has been demonstrated through research on the key point extraction procedure that it is possible to collect enough key points, even in small and smooth sections, by lowering the contrast threshold and scaling the image. Then, a special hierarchical feature point matching method was presented to address the essential matching problem. With ROOTSIFT, a novel iterative localization strategy has been proposed to lower the false alarm rate and reliably find the cloned areas with a 99.9% accuracy.

Ethical Approval

This article does not contain any of the authors' research involving humans or animals.

Funding

The authors affirm that no funds, subsidies, or other forms of assistance were used in the preparation of this article.

Conflict of Interest

There are no legitimate financial or non-financial reasons for the authors to expose this content.

Informed Consent

This article does not contain any of the authors' research involving humans or animals.

Authorship Contributions

Conceptualization: Litty Koshy ; Methodology: Litty Koshy ; Formal analysis and investigation: Litty Koshy , Dr.S.Prayla Shyry; Writing - original draft preparation: Litty Koshy ; Writing - review and editing: Litty Koshy ; Resources: Litty Koshy , Dr.S.Prayla Shyry ; Supervisions: Dr.S.Prayla Shyry.

References

[1] X. Pan and S. Lyu, “Region duplication detection using image feature matching,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 857–867, Dec. 2010.

[2] Luca D’Amiano, Davide Cozzolino, Giovanni Poggi and Luisa Verdoliva, “A Patch Match-Based Dense- Field Algorithm for Video Copy–Move Detection and Localization,” IEEE Trans On Circuits and Systems for video technology, vol. 29, no. 3, March 2019.

[3] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, “A SIFT-based forensic method for copy–move attack detection and transformation recovery,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[4] Arandjelović, Relja, and Andrew Zisserman. "Three things everyone should know to improve object retrieval." 2012 IEEE conference on computer vision and pattern recognition. IEEE, 2012.

[5] Mankar, Snigdha K., and Ajay A. Gurjar. "Image forgery types and their detection: A review." International Journal of Advanced Research in Computer Science and Software Engineering 5.4 (2015): 174-178.

[6] Yuanman Li and Jiantao Zhou, “Fast and Effective Image Copy-Move Forgery Detection via Hierarchical Feature Point Matching ,” IEEE Trans. Inf. Forensics Security, vol. 14, no. 5, May 2019

[7] Gopinath, N., Shyry, S.P. Secured: quantum key distribution (SQKD) for solving side-channel attack to enhance security, based on shifting and binary conversion for securing data (SBSD) frameworks. Soft Comput (2022). https://doi.org/10.1007/s00500-022-07479-w.

[8] D. Cozzolino, G. Poggi, and L. Verdoliva, “Efficient dense-field copy-move forgery detection,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 11, pp. 2284–2297, Nov. 2015.

[9] Xufeng Lin and Chang-Tsun Li ,”PRNU-Based Content Forgery Localization Augmented With Image Segmentation”,IEEE Access, December 24, 2020. Page no:222645-222659.

[10] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, “Detection of copy-move forgery in digital images,” in Proc. Digit. Forensic Res. Workshop, 2003, pp. 1–10.

[11] G. Muhammada, M. Hussain, and G. Bebis, “Passive copy move image forgery detection using undecimated dyadic wavelet transform,” Digit. Invest., vol. 9, no. 1, pp. 49–57, 2012.

[12] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004.

[13] J. Zhao and J. Guo, “Passive forensics for copy-move image forgery using a method based on DCT and SVD,” Forensic Sci. Int., vol. 233, nos. 1–3, pp. 158–166, 2013.

[14] S. Bayram, H. T. Sencar, and N. Memon, “An efficient and robust method for detecting copy-move forgery,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process., Apr. 2009, pp. 1053–1056.

[15] S.-J. Ryu, M. Kirchner, M.-J. Lee, and H.-K. Lee, “Rotation invariant localization of duplicated image regions based on Zernike moments,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1355–1370, Aug. 2013.

[16] M. A. Fischler and R. Bolles, “Random sample consensus: A paradigm for model fitting with applications to image analysis and auto mated cartography,” Commun. ACM, vol. 24, no. 6, pp. 381–395, 1981.

[17] M. Zandi, A. Mahmoudi-Aznaveh and A. Mansouri, “Adaptive matching for copy-move Forgery detection,” IEEE International Workshop on Information Forensics and Security (WIFS), Atlanta, GA, pp. 119-124, 2014.

[18] M. Ghorbani, M. Firouzmand, and A. Faraahi, “DWT-DCT (QCD) based copy-move image forgery detection,” 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), 2011, pp. 1-4.

[19] Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, " ," 2010 IEEE International Conference on Acoustics, Speech and Signal Processing, 2010, pp. 1702-1705, doi: 10.1109/ICASSP.2010.5495485.

[20] S. Lyu and H. Farid, "How realistic is photorealistic?," in IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 845-850, Feb. 2005, doi: 10.1109/TSP.2004.839896.

[21] H. Farid, "Image forgery detection," in IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16-25, March 2009, doi: 10.1109/MSP.2008.931079.

[22] Zhigang Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," in IEEE Transactions on Image Processing, vol. 12, no. 2, pp. 230-235, Feb. 2003, doi: 10.1109/TIP.2002.807361.

[23] Cozzolino, Davide, Giovanni Poggi, and Luisa Verdoliva. "Copy-move forgery detection based on patchmatch." 2014 IEEE international conference on image processing (ICIP). IEEE, 2014.

[24] Bi, Xiuli, and Chi-Man Pun. "Fast copy-move forgery detection using local bidirectional coherency error refinement." Pattern Recognition 81 (2018): 161-175.

[25] Shabanian, Hanieh, and Farshad Mashhadi. "A new approach for detecting copy-move forgery in digital images." 2017 IEEE Western New York Image and Signal Processing Workshop (WNYISPW). IEEE, 2017.

[26] Wang, Xiang-Yang, et al. "A new keypoint-based copy-move forgery detection for small smooth regions." Multimedia Tools and Applications 76.22 (2017): 23353-23382.

[27] Aloraini, Mohammed, Mehdi Sharifzadeh, and Dan Schonfeld. "Sequential and patch analyses for object removal video forgery detection and localization." IEEE Transactions on Circuits and Systems for Video Technology 31.3 (2020): 917-930.

[28] Gopinath, N., and S. Prayla Shyry. "Enhancing the cloud security using side channel attack free QKD with entangled fuzzy logic." Journal of Intelligent & Fuzzy Systems Preprint (2022): 1-11.

[29] Gopinath, N., and S. Prayla Shyry. "Side Channel Attack Free Quantum Key Distribution Using Entangled Fuzzy Logic." Brazilian Journal of Physics 53.2 (2023): 35.

[30] Gopinath, N., and S. Prayla Shyry. "Secured: quantum key distribution (SQKD) for solving side-channel attack to enhance security, based on shifting and binary conversion for securing data (SBSD) frameworks." Soft Computing (2022): 1-8.

[31] Pandey, Ramesh Chand, Sanjay Kumar Singh, and K. K. Shukla. "Passive copy-move forgery detection in videos." 2014 International conference on computer and communication technology (ICCCT). IEEE, 2014.

[32] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou,“An evaluation of popular copy-move forgery detection approaches,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1841–1854,Dec. 2012.