Scale Invariant Fast PHT based Copy-Move Forgery Detection

1st Aroof Aimen
Computer Science and Technology
Central University of Punjab
Bathinda, India
aimenaroof@gmail.com

2nd Amandeep Kaur
Computer Science and Technology
Central University of Punjab
Bathinda, India
aman_k2007@hotmail.com

3rd Sahil Sidheekh
Computer Science and Engineering
Indian Institute of Technology Ropar
Ropar, India
sahil.sidheekh@gmail.com

***Abstract*—Copy-Move forgery is a type of image forgery wherein a patch from the image is copied and pasted on the same image either to increase the occurrence of a particular object or to conceal some important detail in the image. This paper addresses the issue of copy-move forgery using the block-based method of feature extraction. In block-based methods of feature extraction, PHT is one of the competing solutions, but it is not much robust to scaling. This paper proposes Scale-Invariant Fast PHT (SIFPHT) algorithm to detect the copy-move forgery which uses Fast PHT [1] for extracting the features from the blocks. Fast PHT has a higher convergence rate than the traditional PHT, and the results prove that the speed-up of almost 4 is attained for detecting the forgery. Moreover, the Fast PHT features so obtained from the blocks are normalized before comparison due to which the scaled forged segments are also identified. Further, Fast K-Means clustering is used to estimate the similarity in the blocks and hence detect the copy-move forgery.**

***Index Terms*—Copy-Move, PHT, Forgery, Fast PHT, Cluster, Blocks, Features, Images**

I. Introduction

Image forgery is one of the key issues in the current digital world. A mechanism of alteration of the actual images to convey the false meaning is called image forgery. Image forgery is not new. It dates back to 1840 when Hippolyte Bayard, a French photographer produced a fake photo of himself committing suicide due to some frustration. There are two broad domains of detecting the image forgery viz active/intrusive/proactive methods and the passive/non-intrusive/reactive ones [20], [37]. The active method requires prior information about the image. These methods are usually employed at the time of image acquisition by an authorized person and may require special cameras and associated hardware. The important method among the active methods is watermarking wherein the watermark may get distorted if any tempering is done. However, the watermarking tends to degrade the quality of the image as the extra bits are embedded in the image. Therefore the better mechanism is to go for the passive methods which are further split up into various types having one aspect in common, i.e.; no extra efforts are required at the time of image acquisition, liberating the authorizers of the responsibility and preventing the degradation in the quality of the images. The passive methods are also termed as blind forgery detection as the detector has to check the tempered image in every direction to get the clue of the forgery. These passive methods are classified based on camera, pixel, format, source camera identification, physics, and geometry [18]. The camera-based methods are based on the artifacts produced during the acquisition of the image. They include color filter arrays, camera response, etc. The pixel-based methods differentiate pictures, pixel by pixel. Cloning or copy-move forgery, retouching, morphing, splicing, and resampling are some of its types. The format based methods analyze the JPEG compression artifacts. The types include JPEG blocking, JPEG quantization, and Double JPEG. The source camera-based methods deal with camera specifications which may include lens aberration, sensor imperfection, CFA interpolation, etc. In physics-based methods changes in the illumination are observed and in geometric-based methods inconsistency in the location or position of objects is noted. Copy-Move forgery (CMF) [6] is a pixel-based image forgery technique wherein a patch from the image is copied and pasted on the same image either to increase the occurrence of a particular object or to conceal some important detail in the image. This type of forgery is very difficult to detect as the overall homogeneity of the image is restored. It is because the noise acts as an inherent watermark to the image and if the image is tempered, the noise components get distorted indicating forgery. But in the case of Copy-Move forgery the copied segment belongs to the same image and hence the noise components of this segment are in correspondence with the entire image and hence the overall homogeneity of the image is maintained, despite the forgery. The techniques of detecting copy-move forgery include block-based [2] and key point-based [7] methods. In the case of block-based methods, an image is divided into super-imposed or non-super-imposed blocks of suitable size, and then the feature vectors are extracted. These feature vectors could also be extracted by intensity-based, frequency-based, or moment-based methods. There is a drawback associated with either of these methods. In block-based methods, the feature vectors are directly extracted from the blocks which make the size of feature vectors large, and hence the dimension reduction step becomes a necessity. Key-point based methods have a good detection rate of duplicate regions, but they struggle in detecting the forgery in flat regions like ocean, sky, etc.

The various steps carried under copy-move forgery detection (CMFD) procedure are:

- **Preprocessing:** Various tasks like converting an image from color to grayscale, resizing, reducing dimensions, low-pass filtering (LPF), etc. are carried out in this step.
- **Feature Extraction:** This step includes extraction of features using any of the feature extraction techniques.
- **Matching:** The feature vectors are sorted by various sorting schemes like radix sort, lexicographical sort, etc. The similar feature vectors obtain consecutive positions and hence are easy to detect.
- **Filtering:** There may be many false matches especially in flat areas like sky, sea, etc. Filtering uses various morphological operations to reduce such false matches. This procedure is carried by choosing the threshold carefully as too little threshold may lead to many false matches, and too greater threshold may lead to skipping of the forged blocks or key points.

This paper is organized as follows. Section 1 gives a brief overview of image forgery and copy-move forgery in particular. Section 2 gives the related work and section 3 contains the preliminaries like polar harmonic transform, fast polar harmonic transform, and clustering that are prerequisites to the proposed method. Section 4 explains the proposed algorithm and section 5 lists the qualitative and quantitative results obtained. Section 6 concludes the paper with future work in this direction.

II. RELATED WORK

The feature extraction methods of copy-move forgery detection (CFMD) could be classified based on domain into transform domain-based and spatial domain-based methods [42]. Authors in [10], [11] and [47] studied various techniques of detecting image forgery. The spatial domain-based techniques are further divided into moment, key-point, and spatial structure-based techniques. The moment invariants are used to detect various post-processing geometric operations. Authors of [13] used ZM's (Zernike Moments), PZM's (Pseudo Zernike Moments), and OFMM's (Orthogonal Fourier Mellin Moments) for pattern recognition but these moments have inherently complex kernels. The usage of OFMM's and ZM's was compared in [12] and it was observed that although OFMM's are suitable for images of high variability, and ZM's are suitable for the images of low variability but making OFMM's and ZM's scale-invariant may cause degradation in the extracted features. Rotate-Move Forgery using ZM's is detected in [14] but it is observed that ZM's are not scale-invariant. In the key-point based methods, the image is divided into key points and feature vectors are calculated for those key points. Author of [7] gave the concept of Scale-Invariant Feature Transform SIFT and SIFT was used for detecting CMF in [15], [44], [45]. But the problem with SIFT is that it is not much robust to the rotation. Further, copy-move forgery by using Angular Radial Partitioning and Harris Key-Points is detected in [16]. [38] aims to detect CMF in smooth regions in which key-point based techniques fail. The input images are subjected to dynamic histogram equalization (DHE) to improve the contrast and SURF (speeded-up robust feature) is used to extract the features. SURF alone fails to detect CMF in smooth and small regions. So, mDBSCAN (modified density Based Algorithm) was used to detect CMF in such small and smooth regions. SURF uses a computationally expensive approximation of second-order Hessian. The human visual system interprets the image in the form of texture. To handle the geometric operations, authors of [17] put forward local binary pattern (LBP) based method for feature extraction but LBP is not able to detect regions rotated at arbitrary angles.

In the transform-based techniques, few coefficients of the block carry most of the energy of the block. Frequency-based techniques fall into the category of transform domain techniques. A review of various frequency-based solutions for CMFD was done in [18]. DCT (Discrete Cosine Transform) was proposed in [6]. Although this technique is robust against retouching and jpeg compression yet this method cannot make a difference between a forged block and a large texture area like sky etc. which may occur naturally. CMF was detected using DCT in [43].The dimension reduction based techniques reduce the dimensions of feature vectors in frequency-based techniques. CMF was detected by using wavelets and log-polar mapping in [19]. Matching takes place in the LL sub-band only. This approach is effective for small-sized images but impractical for large-sized images. Authors of [20] used both LL and HH bands for detecting CMF and DyWT (Dyadic Wavelet Transform) is proposed in [21] which made DWT (Discrete Wavelet Transform) scale-invariant. Rotation resistant method of detecting CMF using multi-directional, multi-resolutional decomposition was proposed in [37]. DWT-DCT Quantized Coefficient Decomposition (QCD) was proposed in [22] because of which the dimensions of feature vectors were reduced. But this method cannot detect the segment that has undergone post-processing operations like rotation, scaling, heavy compression, etc. Authors of [23] also reduced the feature vectors in DCT by using low-frequency components and CMF detection was improved using quantized DCT coefficients in [40]. The automatic threshold values for test images were generated in [41] using DCT-phase and Benford's law. Fourier Mellin Transform (FMT) based method of feature extraction was proposed in [24] and authors in [25] proposed DAFMT (Discrete Analytical Fourier-Millin transform) for detecting CMF. Locality sensitive hashing (LSH) for approximate nearest neighbor searching was proposed in [27]. PHT technique for invariant image representation was proposed in [2] and [26] used PHT for detecting CMF. Although, PHT is robust to Additive-White Gaussian Noise (AWGN), region shear, partial affine transform JPEG compression, and rotation yet it is not much robust to scaling. Polar Harmonic Transforms was used for image watermarking in [28]. Authors of [1] increased the speed of polar harmonic transforms. Similarly, [29] used a kernel-based method to increase the speed of PHT. Radon transforms together with PCET was used in [30] to attain rotation and scale in-variance together with the robustness against AWGN. Authors of [32] and [33] incorporated quaternion geometry in Bessel-Fourier Moments, Radial Harmonic Fourier, Polar Complex Exponential Transform (PCET) respectively and hence made these techniques applicable to color images. Quaternion geometry was also used in [48] and [49] to detect copy-move forgery.

Triangular inequality was used in [3] to increase the speed of the conventional K-Means clustering algorithm. K-Means clustering is used in [46] and fast K-Means clustering in addition to DCT is used in [4] to detect copy-move forgery. The later detects the forgery at a very rapid rate. Also, two levels of clustering were used to detect CMF in [50]. Authors of [34] and [35] have combined the block and key-point based techniques of copy-move forgery detection using SIFT, DyWT, and SIFT, DWT respectively. Authors in [39] have also leveraged both block and key-point based feature extraction by proposing combined features using LIOP (Local Intensity Order Pattern) and SIFT to detect the CMF even in the regions with few key-points. [36] has introduced Color Fourier Millen Moments, so that the descriptors of color images may be extracted.

Our work is different from [1] in terms of the application. [1] gives the theoretical concept of improving the speed of PHT by using recursion and clustering pixels in 8 radially symmetric octants, however, we extract the features from the images using this theoretical concept and then detect copy-move forgery by Fast K-Means clustering. [4] also has a close relevance with our work, but we have used fast polar harmonic transform to extract the features rather than discrete cosine transform. The contributions of the proposed algorithm (Scale Invariant Fast PHT based Copy-Move Forgery Detection; SIFPHT) for detecting copy-move forgery are as follows:

- The proposed algorithm SIFPHT gains the speed-up of 4 in detecting the copy-move forgery than the baseline PHT [2].
- Both baseline and the SIFPHT are robust to AWGN, region shear, partial affine transform, JPEG compression, and rotation but unlike baseline, SIFPHT is robust to scaling transformations too.
- The forged regions of regular as well as irregular shapes can be detected.

.

III. PRELIMINARIES

A. Polar Harmonic Transform (PHT)

PHT is the representation of waves [2]. It is defined on the unit circle with orthogonality invariant property. So, it is robust to AWGN (additive white Gaussian noise), region shear, partial affine transform JPEG compression, and rotation. The Computational Complexity of PHT is

$$H_{n,l}(r,\theta) = e^{i2\pi nr^2} e^{il\theta} = e^{i(2\pi r^2 + l\theta)} \tag{1}$$

where $H_{n,l}(r,\theta)$ is the kernel of PHT, n is the order and l is the repetition. PHT has an inherent rotation in-variance property because the magnitude of the coefficients does not alter during the rotation.

$$M^r_{nl} = M_{nl}.e^{il\phi} \tag{2}$$

$$|M_{nl}| = |M^r_{nl}| \tag{3}$$

M_{nl} are the PHT coefficients of the image and M^r_{nl} are the PHT coefficients of the rotated image. Also, PHT can estimate the orientation of the image by,

$$M'_{nl} = M_{nl}.e^{-il\phi} \tag{4}$$

$$\phi = \frac{1}{l} arg \frac{M_{nl}}{M'_{nl}} \tag{5}$$

B. Fast Polar Harmonic Transform (Fast PHT)

To decrease the computations of PHT authors in [1] used recursion in the evaluation of angles such that the larger angle can be computed in the form of small pre-computed angles as follows:

$$\cos((m+1)\theta) = \cos(\theta)\cos(m\theta) - \sin(\theta)\sin(m\theta) \tag{6}$$

$$\sin((m+1)\theta) = \sin(\theta)\cos(m\theta) + \cos(\theta)\sin(m\theta) \tag{7}$$

Also clustering of pixels was done in 8 radially symmetric octants. When the clustering procedure was applied, an increase in the speed by the factor of 3-4 was witnessed.

C. Clustering

Clustering is the technique in which the data points are divided into sub-sets such that each data point belongs to one sub-set. K-Means clustering algorithm starts by choosing k centers randomly at some distance apart. Then the data points are mapped to the corresponding centers based on the minimum distance factor. The process of choosing new centers and membership is iterative and in each iteration mean square error is reduced. So the k-centers of clusters tend to drift from their positions until either they stabilize, i.e., do not change their values further or reach to a certain threshold. Fast K-Means algorithm is a variation of the original K-Means clustering algorithm wherein the speed of clustering is higher than conventional K-Means algorithm. This technique aims to reduce the redundant computations done by the original K-Means [3]. The idea is if the data point is too near to some i^{th} center, then there is no meaning in finding the exact distance between this data point and the i^{th} center because anyways it would map to the i^{th} center only. Same is the case if the data point is too far from any i^{th} center, then the exact distance between the data point and the i^{th} center is not required, as anyways it would not map to the i^{th} center. Fast K-Means clustering also uses triangular inequality to increase the speed of the original K-Means algorithm.

IV. PROPOSED ALGORITHM SIFPHT

In this paper, we leverage the concepts of Fast-PHT [1] in extracting features and Fast K-Means clustering algorithm [3] in detecting the similar/forged clusters. The intention is to detect the copy-move forgery at a rapid rate. Also, this forgery detection is scale invariant as the image blocks are normalized before comparison. The overview of the proposed algorithm SIFPHT is given in the flowchart and is in accordance with Algorithm 1 and 2.

In Algorithm 1, the color image is first converted to gray-scale image, and then this image is divided into the overlapping blocks. The features are extracted from these blocks using Fast PHT (Algorithm 2). These features are then normalized and fed to the Fast K-Means Clustering algorithm [3] which outputs the clusters/classes. Then, blocks of each class are sorted and correlation is found between the adjacent pairs of blocks, which if greater than threshold Th are checked further for similarity. The last step is to check whether the distance between so obtained sorted blocks is greater than neighboring distance N_d; if so then the blocks are labeled as similar. The step-wise detailed explanation of the algorithm is given as follows.

Algorithm 1: SIFPHT_CMFD(Input_Image= RGB Image)

```
Input: RGB image of size ma × na
gray_image= 0.228R + 0.587G+ 0.114B
Divide image in the blocks of b0 × b0
All_blocks ← (ma−b0 + 1) × (na−b0 + 1)
for block in All_blocks do
    features ← Fast_PHT(block)
    normalized_features[block] ← Normalize(features)
end
classes← Fast K-means (All_blocks)
for class in classes do
    s_blks ← Radix_Sort(All_blocks)
    for b in s_blks do
        corr ← correlation(s_blks[b], s_blks[b + 1])
        if corr ≥ Th then
            if d(s_blks[b], s_blks[b + 1]) ≥ N_d then
                Label b, b + 1 as similar
            end
        end
    end
end
```

Algorithm 2: Fast_PHT (Block= *block*, *order*=*n*, *repetition*=*m*)

```
Input: block of size b0 × b0
for pixel in the block do
    Compute angular and radial parts of the PHT
      recursively
    Cluster 8-way symmetric/anti-symmetric pixels
end
Output features of block
```

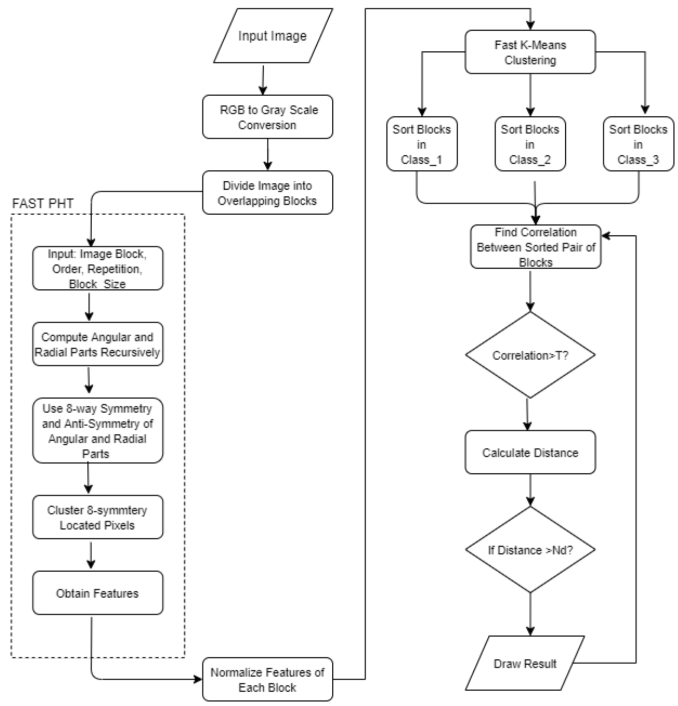
A. Algorithm

Algorithm: To detect copy-move forgery.

Input: An image of size $ma \times na$.

Output: The forgery detected image of size $ma \times na$.

- **Step I:** It is the pre-processing step where the input color image is converted to the gray-scale image and is divided into overlapping blocks of fixed size. The block size and overlap are set as per the best result obtained and are different for different images.



Flowchart of SIFPHT

- **Step II:** A Fast PHT (Algorithm 2) [1] is used to extract the features from the overlapped blocks which uses recursion in the evaluation of angles such that the larger angle can be computed in the form of small pre-computed angles.

  The angular function is given as

$$e^{jm\theta} = \cos(m\theta) + j\sin(m\theta) \tag{8}$$

The recursive equations are:

$$\cos((m+1)\theta) = \cos(\theta)\cos(m\theta) - \sin(\theta)\sin(m\theta) \tag{9}$$

$$\sin((m+1)\theta) = \sin(\theta)\cos(m\theta) + \cos(\theta)\sin(m\theta) \tag{10}$$

where $m = 0, 1, ., m_{max}$ is the repetition, $r = \sqrt{x_i^2 + y_k^2}$, (i, k) is the pixel location and $\cos(\theta) = \dfrac{x_i}{r}$ and $\sin(\theta) = \dfrac{y_k}{r}$.

The radial function is given as

$$e^{j2\pi nr^2} = \cos(2\pi nr^2) + j\sin(2\pi nr^2) \tag{11}$$

where n is the order. For $n > 1$ we have

$$\cos(2\pi r^2(n+1)) = \cos(2\pi r^2)\cos(2\pi r^2 n) - \sin(2\pi r^2)\sin(2\pi r^2 n) \tag{12}$$

$$\sin(2\pi r^2(n+1)) = \sin(2\pi r^2)\cos(2\pi r^2 n) + \cos(2\pi r^2)\sin(2\pi r^2 n) \tag{13}$$

where $n = 0, 1, ., n_{max}$
Clustering of pixels using 8-way symmetry or anti-symmetry properties of angular and radial parts of kernel functions is done. The coordinates of the pixels

are $P1(i,k)$, $P2(k,i)$, $P3(-k-1,i)$, $P4(-i-1,k)$, $P5(-i-1,-k-1)$, $P6(-k-1,-i-1)$, $P7(k,-i-1)$, $P8(i,-k-1)$. These pixels share the same centre.

$$\mathrm{A}_{nm} = \frac{4\lambda}{N^2}\sum_{i=0}^{N-1} f(i,k) \times [\{\cos(2\pi n r_{jk}^2)\cos(m\theta_{jk}) - \sin(2\pi n r_{jk}^2)\sin(m\theta_{jk})\} - j\{\sin(2\pi n r_{ik}^2)\cos(m\theta_{ik}) + \cos(2\pi n r_{ik}^2)\sin(m\theta_{ik})\}] \tag{14}$$

where $r = \sqrt{x_i^2 + y_k^2}$ and $\theta_{ik} = tan^{-1}(y_k/x_i)$. The eight point symmetry/ anti-symmetry leads to the following equation.

$$\mathrm{A}_{nm} = \frac{4\lambda}{N^2}\sum_{i=0}^{R-1}\sum_{k=0}^{l}[\{F_1\cos(m\theta_{ik}) + F_2\sin(m\theta_{ik})\}\cos(2\pi n r_{ik}^2) - \{F_3\cos(m\theta_{ik}) + F_4\sin(m\theta_{ik})\}\sin(2\pi n r_{ik}^2)] - j[\{F_1\cos(m\theta_{ik}) + F_2\sin(m\theta_{ik})\}\sin(2\pi n r_{ik}^2) + \{F_3\cos(m\theta_{ik}) + F_4\sin(m\theta_{ik})\}\cos(2\pi n r_{ik}^2)] \tag{15}$$

where $x_i = (2i+1)/N$, $y_k = (2k+1)/N$

The clustered feature vectors for each block are returned by Fast_PHT (Algorithm 2).

- **Step III:** The features obtained from Fast PHT are normalized to the scale of 0-1.
- **Step IV:** Fast K-Means Clustering [3] is used to sort the blocks into classes or clusters. This clustering technique aims to reduce the redundant computations done by the original K-Means. Fast K-Means clustering uses triangular inequality to increase the speed of original K-Means algorithm by avoiding unnecessary calculations.
- **Step V: Detection of duplicated regions** For each class, extracted block feature vectors are sorted using radix sort and the correlation between the pair of radix sorted blocks is computed. Let As be a sorted matrix, then each row of this sorted matrix is compared with the other row i.e. row $As(i)$ is compared with row $As(i+1)$ where i represents the index. Correlation between sorted blocks is calculated by the formula,

$$correlation = \frac{\sum_{i=1}^{n}(pxi - \bar{px}).(pyi - \bar{py})}{\sqrt{\sum_{i=1}^{n}(pxi - \bar{px})^2.(pyi - \bar{py})^2}} \tag{16}$$

Where px and py are Fast PHT coefficients and $\bar{px}$ and $\bar{py}$ are the corresponding means and n is the number of coefficients in the block.

- **Step VI: Post Processing** If the correlation is greater than the similarity_threshold, then the Euclidean distance $D(i)$ between these similar blocks is computed to eliminate the False Positives $(FP's)$. If $D(i)$ is greater than neighboring distance Nd (manually set), then two blocks are labeled as similar. Then, this procedure repeats for other blocks.

TABLE I

PARAMETERS FOR DETECTING FORGERY IN TRANSLATED TEST_IMAGE 1 AND TRANSLATED AND SCALED TEST_IMAGE 2

Parameters	Test_Image 1	Test_image 2
Block Size	20	30
Overlap	8	14
Nd	60	20
Threshold	0.999	0.9999
S_Threshold	0.08	0.09
Runtime Fast PHT	9.218952742540774	NA
Runtime PHT	32.6409	NA

V. RESULTS AND DISCUSSIONS

The performance of the proposed algorithm SIFPHT was evaluated using [8], [9] and [5] data-sets. The proposed, as well as the, existing algorithm has been implemented in Matlab R2013a on the Microsoft Windows environment on a PC with processor Intel (R) Core (TM) i7-3520 CPU, 8 GB RAM and 64-bit operating system.

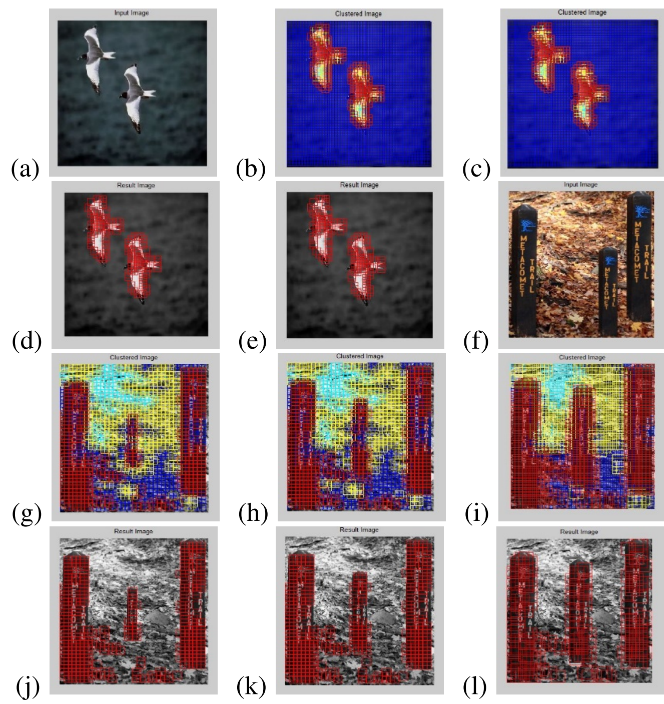


Fig. 1. **[left to right] (a)** is the input Test_image 1 on which the proposed algorithm is applied **(b and c)** are the clustered images obtained due to Fast PHT and PHT respectively **(d and e)** are the forgery detected images obtained due to Fast PHT and PHT respectively **(f)** Input Test_Image 2 for Fast PHT scale performance check. **(g-i)** Clustered Test_Image 2 scaled to 40, 60 and 80% respectively **(j-l)** Output Test_Image 2 showing performance of Fast PHT for 40, 60 and 80% scaling respectively.

The authentic images from [5] dataset were forged manually in Paint Shop. About 50 images were taken into consideration. The visual results (Figure 1) obtained indicate that the proposed technique is efficient in detecting the copy-move forgery. Both PHT and Fast PHT used together with Algorithm 1 are capable of detecting the forged blocks (Figure 1 a-e). (Figure 1 f-l) shows that the proposed technique is robust to scaling and detects forgery even if the forged segment

TABLE II
PERFORMANCE METRICS

Metrics	Value
True Positive	48
False Positive	1
False Negative	1
Precision	0.97959
Recall	0.97959
F_Measure	0.97959

TABLE III
AVERAGE PARAMETER VALUES OBTAINED

Parameters	Values
Average Block Size	38.44 40
Average Overlap	11.58 12
Average Nd	49.4
Average Threshold	0.98984
Average S_Threshold	0.791429

undergoes scaling of 40, 60 or even 80%. Also, Table 1 indicates that the Fast-PHT technique of feature extraction is swifter than the conventional PHT feature extraction technique by the factor of 4. The quantitative parameters obtained in Table 2 indicate that the proposed algorithm is efficient and has the precision, recall, and F_Measure of 0.97959. Further, the average values of predefined parameters are estimated. From Table 3, it is estimated that the average block size of 40, the overlap of 12, Nd 14.4, threshold 0.98984 and S_Threshold 0.791429 are optimal for detecting copy-move forgery.

VI. CONCLUSION AND FUTURE WORK

Copy-move forgery involves copying of a segment of an image and pasting it on the same image, either to hide some detail or to increase the frequency of the certain object. In this paper, first, an image is divided into overlapping blocks then a Fast-PHT transform technique is used to extract the features from each block. Fast K-Means algorithm is used to sort similar blocks into classes. Then the correlation between the sorted blocks is compared with the predefined threshold. If the condition is satisfied, then the Euclidean distance between the sorted blocks is compared with predefined distance, Nd. In the end, clusters are formed for similar-looking objects thereby detecting forgery.

The results obtained depict that the Fast-PHT technique of feature extraction is swifter than the conventional PHT feature extraction technique by the factor of 4. Results also show that the proposed technique SIFPHT is robust to scaling and detects forgery even if the forged segment undergoes scaling of 40, 60 or even 80%. The future work in this direction lies in proposing a technique that would be able to differentiate between the identical objects in an image and the forged objects in an image and detecting the copy-move forgery in videos.

REFERENCES

[1] Singh, C., Kaur, A. (2015). Fast computation of polar harmonic transforms.Journal of Real-Time Image Processing,10(1), 59-66. doi:10.1007/s11554-012-0252-y

[2] Yap, P. T., Jiang, X., Kot, A. C. (2010). Two-dimensional polar harmonic transforms for invariant image representation.IEEE Transactions on Pattern Analysis and Machine Intelligence,32(7), 1259-1270.

[3] Elkan, C. (2003). Using the triangle inequality to accelerate k-means. In-Proceedings of the 20th International Conference on Machine Learning (ICML-03)(pp. 147-153). doi:10.1109/tpami.2009.119

[4] Fadl, S. M., Semary, N. A. (2014, December). A proposed accelerated image copy-move forgery detection. InVisual Communications and Image Processing Conference, 2014 IEEE(pp. 253-257). IEEE. doi:10.1109/vcip.2014.7051552

[5] Dataset CASIA.v1.0 is available at https://www.kaggle.com/sophatvathana/casia-dataset?

[6] Fridrich, A. J., Soukal, B. D., Lukáš, A. J. (2003). Detection of copy-move forgery in digital images. Inin Proceedings of Digital Forensic Research Workshop.

[7] Lowe, D. G. (1999). Object recognition from local scale-invariant features. InComputer vision, 1999. The proceedings of the seventh IEEE international conference on(Vol. 2, pp. 1150-1157). IEEE. doi: 10.1109/ICCV.1999.790410

[8] Cozzolino, D., Poggi, G., Verdoliva, L. (2014, October). Copy-move forgery detection based on patchmatch. In Image Processing (ICIP), 2014 IEEE International Conference on(pp. 5312-5316). IEEE.

[9] Ardizzone, E., Bruno, A., Mazzola, G. (2015). Copy–move forgery detection by matching triangles of keypoints. IEEE Transactions on Information Forensics and Security, 10(10), 2084-2094.

[10] Farid, H. (2009). Image forgery detection. IEEE Signal processing magazine, 26(2), 16-25.

[11] Birajdar, G. K., Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. Digital Investigation, 10(3), 226-245.

[12] Kan, C., Srinath, M. D. (2002). Invariant character recognition with Zernike and orthogonal Fourier–Mellin moments. Pattern recognition, 35(1), 143-154.

[13] Flusser, J., Zitova, B., Suk, T. (2009). Moments and moment invariants in pattern recognition. John Wiley Sons.

[14] Ryu, S. J., Lee, M. J., Lee, H. K. (2010, June). Detection of Copy-Rotate-Move Forgery Using Zernike Moments. In Information hiding (Vol. 6387, pp. 51-65).

[15] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G. (2011). A SIFT-based forensic method for copy–move attack detection and transformation recovery. IEEE Transactions on Information Forensics and Security, 6(3), 1099-1110.

[16] Uliyan, D. M., Jalab, H. A., Abdul Wahab, A. W., Sadeghi, S. (2016). Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points. Symmetry, 8(7), 62.

[17] Li, L., Li, S., Zhu, H., Chu, S. C., Roddick, J. F., Pan, J. S. (2013). An efficient scheme for detecting copy-move forged images by local binary patterns. Journal of Information Hiding and Multimedia Signal Processing, 4(1), 46-56.

[18] Dixit, A., Gupta, R. K. (2016). Copy-Move Image Forgery Detection using Frequency-based Techniques: A Review. International Journal of Signal Processing, Image Processing and Pattern Recognition, 9(3), 71-88.

[19] Myna, A. N., Venkateshmurthy, M. G., Patil, C. G. (2007, December). Detection of region duplication forgery in digital images using wavelets and log-polar mapping. In Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on (Vol. 3, pp. 371-377). IEEE.

[20] Zhang, J., Feng, Z., Su, Y. (2008, November). 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.

[21] Muhammad, G., Hussain, M., Khawaji, K., Bebis, G. (2011, July). Blind copy move image forgery detection using dyadic undecimated wavelet transform. In Digital Signal Processing (DSP), 2011 17th International Conference on (pp.1-6). IEEE.

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

[23] Cao, Y., Gao, T., Fan, L., Yang, Q. (2012). A robust detection algorithm for copy-move forgery in digital images. Forensic science international, 214(1), 33-43.

[24] Bayram, S., Sencar, H. T., Memon, N. (2009, April). 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.
[25] Zhong, J., Gan, Y. (2016). Detection of copy–move forgery using discrete analytical Fourier–Mellin transform. Nonlinear Dynamics, 84(1), 189-202.
[26] Li, L., Li, S., Wang, J. (2012, October). Copy-move forgery detection based on PHT. In Information and Communication Technologies (WICT), 2012 World Congress on (pp. 1061-1065). IEEE.
[27] Li, Y. (2013). Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic science international, 224(1), 59-67.
[28] Li, L., Li, S., Abraham, A., Pan, J. S. (2012). Geometrically invariant image watermarking using Polar Harmonic Transforms. Information Sciences, 199, 1-19.
[29] Hosny, K. M., Darwish, M. M. (2016). A Kernel-Based method for Fast and accurate computation of PHT in polar coordinates. Journal of Real-Time Image Processing, 1-13.
[30] Singh, S. P., Urooj, S. (2015). Combined rotation-and scale-invariant texture analysis using radon-based polar complex exponential transform. Arabian Journal for Science and Engineering, 40(8), 2309-2322.
[31] Shao, Z., Shu, H., Wu, J., Chen, B., Coatrieux, J. L. (2014). Quaternion Bessel–Fourier moments and their invariant descriptors for object reconstruction and recognition. Pattern Recognition, 47(2), 603-611.
[32] Xiang-yang, W., Wei-yi, L., Hong-ying, Y., Pan-pan, N., Yong-wei, L. (2015). Invariant quaternion radial harmonic Fourier moments for color image retrieval. Optics Laser Technology, 66, 78-88.
[33] Wang, X. Y., Li, W. Y., Yang, H. Y., Wang, P., Li, Y. W. (2015). Quaternion polar complex exponential transform for invariant color image description. Applied Mathematics and Computation, 256, 951-967.
[34] Hashmi, M. F., Anand, V., Keskar, A. G. (2014). Copy-move image forgery detection using an efficient and robust method combining undecimated wavelet transform and scale invariant feature transform. Aasri Procedia, 9, 84-91.
[35] Pun, C. M., Yuan, X. C., Bi, X. L. (2015). Image forgery detection using adaptive over segmentation and feature point matching. IEEE Transactions on Information Forensics and Security, 10(8), 1705-1716.
[36] Mennesson, J., Saint-Jean, C., Mascarilla, L. (2014). Color Fourier–Mellin descriptors for image recognition. Pattern Recognition Letters, 40, 27-35.
[37] Qiao, M., Sung, A., Liu, Q., Ribeiro, B. (2011, November). A novel approach for detection of copy-move forgery. In proceedings of Fifth International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP 2011) (pp. 44-47).
[38] Bilal, M., Habib, H. A., Mehmood, Z., Yousaf, R. M., Saba, T., Rehman, A. (2020). A robust technique for copy-move forgery detection from small and extremely smooth tampered regions based on the DHE-SURF features and mDBSCAN clustering. Australian Journal of Forensic Sciences, 1-24.
[39] Lin, C., Lu, W., Huang, X., Liu, K., Sun, W., Lin, H., Tan, Z. (2019). Copy-move forgery detection using combined features and transitive matching. Multimedia Tools and Applications, 78(21), 30081-30096.
[40] Zhang, Z., Wang, D., Wang, C., Zhou, X. (2017). Detecting Copy-move Forgeries in Images Based on DCT and Main Transfer Vectors. KSII Transactions on Internet Information Systems, 11(9).
[41] Ustubioglu, B., Ulutas, G., Ulutas, M., Nabiyev, V. V. (2016). A new copy move forgery detection technique with automatic threshold determination. AEU-International Journal of Electronics and Communications, 70(8), 1076-1087.
[42] Soni, B., Das, P. K., Thounaojam, D. M. (2017). CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection. IET Image Processing, 12(2), 167-178.
[43] Alkawaz, M. H., Sulong, G., Saba, T., Rehman, A. (2018). Detection of copy-move image forgery based on discrete cosine transform. Neural Computing and Applications, 30(1), 183-192.
[44] Chen, C. C., Lu, W. Y., Chou, C. H. (2019). Rotational copy-move forgery detection using SIFT and region growing strategies. Multimedia Tools and Applications, 78(13), 18293-18308.
[45] Yang, B., Sun, X., Guo, H., Xia, Z., Chen, X. (2018). A copy-move forgery detection method based on CMFD-SIFT. Multimedia Tools and Applications, 77(1), 837-855.
[46] Al-Qershi, O. M., Khoo, B. E. (2019). Enhanced block-based copy-move forgery detection using k-means clustering. Multidimensional Systems and Signal Processing, 30(4), 1671-1695.
[47] Zhang, Z., Wang, C., Zhou, X. (2018). A Survey on Passive Image Copy-Move Forgery Detection. Journal of Information Processing Systems, 14(1).
[48] Wang, X. Y., Liu, Y. N., Xu, H., Wang, P., Yang, H. Y. (2018). Robust copy–move forgery detection using quaternion exponent moments. Pattern Analysis and Applications, 21(2), 451-467.
[49] Thajeel, S. A., Mahmood, A. S., Humood, W. R., Sulong, G. (2019). Detection Copy-Move Forgery in Image Via Quaternion Polar Harmonic Transforms. KSII Transactions on Internet and Information Systems (TIIS), 13(8), 4005-4025.
[50] Abdel-Basset, M., Manogaran, G., Fakhry, A. E., El-Henawy, I. (2018). 2-Levels of clustering strategy to detect and locate copy-move forgery in digital images. Multimedia Tools and Applications, 1-19.