Gray Level Co-occurrence Matrix with Binary Robust Invariant Scalable Keypoints for Detecting Copy Move Forgeries

Amarpreet Singh and Sanjogdeep Singh*

Amritsar Group of Colleges, Amritsar, India; Email: amarpreet.cse@acetedu.in (A.S.)
*Correspondence: er.sanjogdeep@gmail.com (S.S.)

***Abstract*—With advancement in technology, especially in imaging field, digital image forgery has increased a lot nowadays. In order to counter this problem, many forgery detection techniques have been developed from time to time. For rapid and accurate detection of forged image, a novel hybrid technique is used in this research work that implements Gray Level Co-occurrence Matrix (GLCM) along with Binary Robust Invariant Scalable Keypoints (BRISK). GLCM significantly extracts key attributes from an image efficiently which will help to increase the detection accuracy. BRISK is known to be one of the 3 fastest modes of detection which will increase the execution speed of GLCM. BRISK even processes scaled and rotated images. Then the Principal Component Analysis (PCA) algorithm is applied in the final phase of detection will remove any unrequited element from the scene and highlights the concerned forged area.**

***Keywords*—copy-move forgery, Discrete Wavelet Transform (DWT), Gray Level Co-occurrence Matrix (GLCM), general architecture, image manipulation**

I. Introduction

Image forensics' objective is to identify the legitimacy and source of digital photographs without the assistance of an embedded security system. One of the most actively researched subtopics in this subject is certainly Copy-Move Forgery Detection (CMFD). A copy-move forgery is a name given to an image that has had some of its content copied and pasted into another region of the same picture. Common motives include hiding a feature in the image or emphasising certain elements. A copy-move fake is simple to produce. Furthermore, as the source area and the target area are both parts of a single image, so characteristics like color intensity [1], lighting, and noise are anticipated to be closely aligned between the manipulated and the original region.

A major tool in digital picture recognition is copy-move forgery detection that has emerged as a hot topic of research in recent years as it relates to the reliability and legitimacy of photographs (CMFD). Because the tampered section is reproduced from a single photograph, CMFD's objective is to identify regions that are similar to other regions of the image. Geometric or post-processing procedures are typically performed upon manipulated parts during the tampering process to render the forgery genuine and undetectable. The key piece of evidence in CMFD is the striking resemblance between the manipulated parts and the original zones [2].

Broadly, the two categories are utilized to carry out operations on the image depending upon the type of a forgery. The categories are shown in Fig. 1 below.

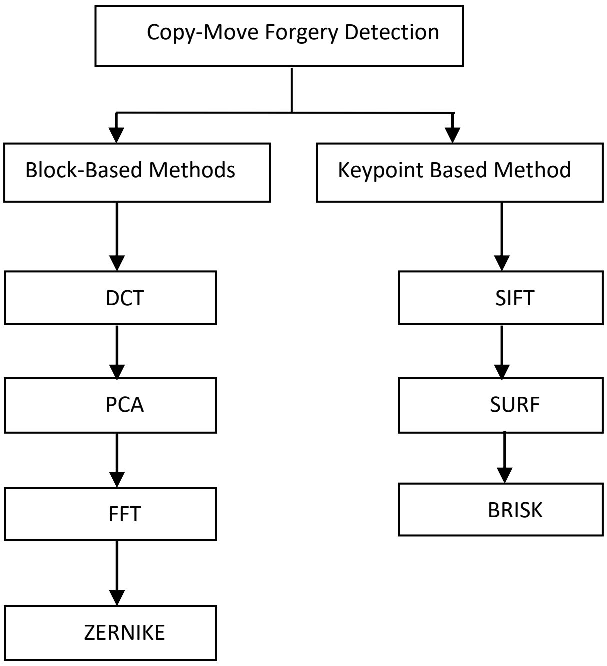

Figure 1. Categories of CMFD techniques.

The following information is more pertinent to the pipeline's steps:

1) Pre-processing: Pre-processing is the preliminary step, which includes certain conversion, transformation or decomposing procedures. Preparing and representing data such that the upcoming feature extraction phase is as effective as possible is the aim of the pre-processing phase. The two simplest but also most crucial pre-processing techniques are colour space conversion and

Manuscript received October 18, 2022; revised November 28, 2022, accepted December 11, 2022.

doi: 10.18178/joig.11.1.82-90

grayscale conversion, which turn RGB pixels into grayscale images with a 0 to 255 colour spectrum (e.g., RGB to HSV, or RGB to YCbCr [3]). Two process options occur based on the initial image. Either keypoint-based or block-based CMFD approaches are available. The photos can be pre-processed in both scenarios. For instance, because most techniques work with grayscale photos, they first need to integrate the colour channels.

2) Feature extraction: One of the most crucial steps that will affect the system's overall accuracy is feature extraction. This step's objective is to provide a collection of concise yet significant data vectors, or "feature descriptors," that represent each component of the target digital image. The feature vectors in the digital photo can be extracted using a variety of methods. The Scale-Invariant Feature Transform (SIFT), first developed by Lowe, is an exceptionally reliable and eminent approach in this field. While, SIFT offers a powerful feature description method that is resistant to scaling and rotation among other difficult transformations, it also comes with a high computing complexity and expense. SIFT may not be the best option for use in actual criminal investigations where a sizable number of digital photos must be checked before being used in trial, despite the identification findings from SIFT appearing to be quite accurate in terms of efficiency [4]. The methods of SIFT keypoint detection and feature extraction have been sped up in numerous experiments. Speeded-up Robust Feature (SURF) is probably the most eminent and effective methods that has been suggested so far. Additionally, several intriguing methods make use of the pre-processing phase to quicken the subsequent SIFT feature extraction procedure.

3) Feature Matching: Feature matching procedures are carried out following the extraction of feature descriptors in the preceding stage. This procedure entails looking for patches or sections of the target image that match and have feature descriptors that are similar. The matching procedure is also a critical step in establishing the CMFD system's total detection performance [5].

4) Filtering: The likelihood of erroneous matches has been decreased through the use of filtering algorithms. For illustration, removing similarities between zones that are geographically adjacent to one another is a frequent active noise cancellation technique. Since neighbouring pixels frequently have comparable brightness which may lead to misleading counterfeit detection. Additionally, several distance thresholds were put forth to weed out unreliable matches. For example, various publications advocated the Euclidean distance between matching feature vectors. Other scholars, however, suggested the correlation coefficient among two feature vectors as a measure of similarity [6].

5) Post-processing: This final phase aims to only keep matches that display same behavioural patterns. Think about a group of matches from a duplicated zone. Within both the target and the source blocks, these matches ought to be situated close to one another (or keypoints). Additionally, matches that result from the identical copy-move operation ought to have an equivalent degree of scalability, rotation, and translation. By requiring a minimal number of similar shift vectors between matches, the most frequent post-processing option manages outliers. The translation (in picture coordinates) between two matched feature vectors is contained in a shift vector. Assume, for instance, a collection of blocks that are straightforward replicas with no scaling or rotation [7]. The shift vectors' histogram subsequently shows a peak at the copy operation's translation constants.

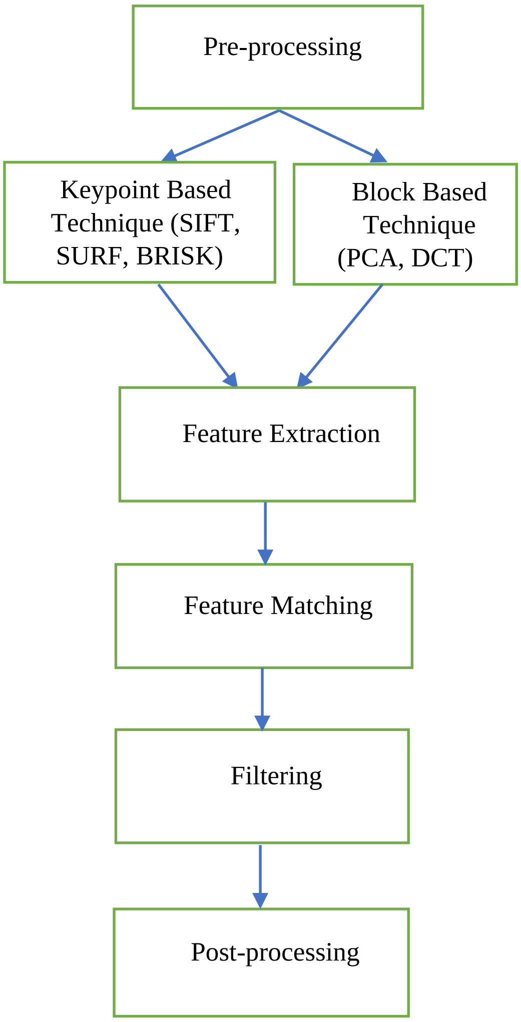
Pre-processing
Keypoint Based Technique (SIFT, SURF, BRISK)
Block Based Technique (PCA, DCT)
Feature Extraction
Feature Matching
Filtering
Post-processing

Figure 2. Common processing pipeline for the detection of copy-move forgeries.

Block-based and keypoint-based strategies can be used to categorise CMFD approaches (Fig. 2). The picture is often divided into small, uniform, and overlapping blocks via block-based algorithms and each block's robust characteristics are extracted. The tampered zones are then produced by labelling the image block after sorting and matching the attributes. The majority of cutting-edge block-based detection techniques make use of the five main categories based on the block technique for feature extraction. Numerous post-processing processes, including compressing, blur, and noise are resistant to frequency domain-based approaches. Due to the DCT and SVD combination, these techniques are resistant to JPEG compression, distortion and noise issues. Frequency-based block characteristics, on the other hand, are modifications of a geometric transformation [8]. Block feature-based approaches will extract numerous local features, which will add significantly to the time consumed. Techniques for reducing dimensionality have been utilised to decrease the retrieved block features' dimension and speed up matching. LBP is a grey-scale texture operator that is applied in Local Binary Pattern (LBP)-based approaches to characterise the spatial configuration of the picture texture. Owing to the use of Hessian points and centre symmetric LBP, these techniques are invariant to translation, scaling, and illumination (CSLBP) [9]. Due to the lack of rotation- and blur-invariant features, this technique is not resistant to blurring and rotation degradation. To segment the zone of interest, texture-based approaches combine statistical analysis and colour texture. Nevertheless, the detection rate of this method drastically decreased if the picture had a high level of blur. Texture-based techniques are not resistant to attacks involving geometric transformations. Moment invariant, which includes blur moment, hue moment, Zernike moment, and other characteristics, is a set of features that are invariant to a geometric transformation in moment invariant-based approaches [10]. Each circular colour block that is overlapping is extracted for its QEM (quaternion exponent moment) moduli. Super pixel concept can be used to lessen the strategy's principal drawback, which is its greater computational complexity. Keypoint based algorithms, in contrast to block-based algorithms, depends on the recognition and selection of high-entropy picture sections, or the "keypoints". Afterward, a feature vector is extracted for each keypoint. Because fewer feature vectors are calculated as a function, feature matching and post-processing computational complexity is decreased. Because there are fewer feature vectors, post-processing thresholds must be smaller than for block-based approaches.

The fact that duplicated zones are frequently only sporadically blanketed by matching keypoints is a disadvantage of keypoint approaches. It is possible that the region will not be duplicated at all if the copied regions lack pattern. Scale Invariant Feature Transform (SIFT) and SURF are two popular keypoints-based CMFD methods. When SIFT was first developed, it was for object recognition. In the area of forgery detection, SIFT is a well-known and still widely used feature descriptor. Finding keypoints (feature points) in various scale spaces and determining their prevailing orientation are the main goals of the SIFT method [11]. Corners, edges, bright spots in dark areas, and dark spots in bright areas are just a few of the very noticeable places that SIFT identified as being the most important and which are unaffected by lighting, linear transformation, or noise. SIFT is made to be resistant to scaling and rotation, and the algorithm works well even when there is noise or variations in lighting. In scale-space representation, the Difference of Gaussian (DoG) is used to identify conspicuous points at various scales [12]. With the addition of DoG, SIFT has considerably decreased the computational complexity of CMFD; however, the quantity of feature vectors created is still quite significant. This would have an effect on the matching phase, particularly for high-resolution photographs. SURF is typically used in computer vision applications like object recognition and picture registration. In addition to maintaining the scaling and rotation invariance of SIFT, SURF, which is based on classical SIFT, is resistant to noise, detecting displacements, and geometric and illumination deformations. By computing the pertinent Hessian matrix and locating the extreme points of scale space, SURF finds keypoints [13]. Rectangular box filters are used by SURF to approximate the Gaussian second-order derivative due to the significant time complexity of computing the image's second-order derivative. Box filters let convolution calculations run more quickly and with less complexity. When it comes to quantitative comparison of most of the studies, a below conclusion is made.

BRISK>SURF>SIFT>AKAZE>KAZE

II. Related Works

Muzaffer [14] suggested a new method to detect the forgery in copy-move. The QD (Quadtree Decomposition) was implemented for segmenting the input image into 2 sub-images. This method allocated 2 labels: smooth and textured on the sub-images. LBPROT technique was employed to offer the textural form of smooth labelled segment. Thereafter, this method helped in extracting the key-points from both segments. The extracted key-points were matched to classify the image as forged or original. The experimental results indicated that the suggested method performed robustly against scaling and rotation assaults.

Liu [15] projected a new model which had two phases for detecting the CMF (copy-move forgery). Initially, the atrous (dilated) convolution was put together with skip matching for augmenting the spatial information and leveraging the hierarchical attributes. Subsequently, Proposal SuperGlue was suggested for eliminating the FA (false-alarmed) regions and remedy imperfect regions. A mechanism was built for enclosing the suspicious areas on the basis of proposal generation and backbone score maps. Eventually, the DL (deep learning) based technique of extracting key-point SuperPoint and matching SuperGlue was exploited to match carry out matching. The experimental outcomes validated that the projected model was effective to detect the forgery in CM (copy-move).

Thakur [16] presented an effectual framework to detect the splicing and CMF (copy-move forgery). The fundamental intend of this framework was to detect the left traces after diverse post-processing operations such as JPEG Compression, insertion of noise, blurring, contrast adjustment etc. After that, a SDMFR (second difference of median filter) was employed on the image and integrated with LFR (Laplacian filter residual) for suppressing the image content. The presented framework was computed on CoMoFoD and BOSSBase datasets. The outcomes exhibited that the presented framework offered accuracy on 95.97% and 94.26% on both datasets respectively while detecting the forgery in copy-move.

Hossein-Nejad [17] introduced a novel feature-based technique with the purpose of detecting the forgery in copy-move. The attributes were extracted using SIFT (scale-invariant feature transform) algorithm. Later, g2NN criteria were considered to perform the matching procedure. At last, this technique deployed an enhanced A-RANSAC to eliminate the mismatches to illustrate the stopping criteria on the basis of number of final matches. The standard A-RANSAC technique was useful for maximizing the execution time and mitigating the speed. MICC-F220 dataset was applied to simulate the introduced technique. The simulation outcomes confirmed the supremacy of the introduced technique over the traditional methods with respect to precision and execution time.

Gan [18] developed a system in which PST (Polar Sine Transform) was integrated with LSH (Locality Sensitive Hashing) for detecting the copy-move forgery image. In the first stage, the system emphasizes on splitting the detected image into several overlapping blocks. After that, the attributes were extracted from every block using PST and classified based on LSH. In the end, Euclidean distance was put forward to post-process the images so that the weak block feature pairs were filtered out. The experimental results reported that the developed system was robust against rotation and JPEG compression and outperformed the existing techniques.

Zheng [19] investigated an algorithm to detect CMF (copy-move forgery) in an image for which the structure tensor and HSV color algorithm was implemented for clustering the feature points. At first, this algorithm aimed at clustering the SIFT (scale-invariant feature transform) feature points on the basis of structure tensor, and dividing all feature points into flat, edge, and corner feature points. At second, HSV color algorithm was implemented to divide feature points into 63 clusters. At last, features were matched in every cluster to employ the similarity of texture and color amid source and tampered area, which resulted in mitigating the time to match the feature and enhance the efficiency of the algorithm. The experimental outcomes revealed the effectiveness of the investigated algorithm for detecting the tampered regions.

Li [20] formulated a fast and effectual algorithm to detect the forgery in copy-move via hierarchical feature point matching. An effective number of key-points were produced when the contrast threshold was alleviated and the input image was rescaled. A new hierarchical matching method was constructed for dealing with the issues related to match the key-points. The FAR (false alarm rate) was lessened and the tampered areas were localized using an innovative iterative localization method relied on robustness properties and the color information about every key-point. The experimental outcomes indicated that the formulated algorithm offered higher efficiency and accuracy.

Zhang [21] established a fusion strategy that combined SF (sparse-field) technique with DF (dense-field) technique. The CST (color space transformation) and adaptive SLIC (Simple Linear Iterative Clustering) algorithm was exploited to pre-process the image. Then, the key-point was extracted and matched through SIFT (scale-invariant feature transform). The next phase focused on extracting the Zernike moments and matching the PatchMatch feature for the above region. The last phase utilized the morphological post-processing in order to localize the tampered area in precise manner. The experimental results revealed that the established strategy performed well.

Jia [22] devised a new technique for detecting CMFs (copy-move forgeries) in frame relied on requirements. This technique constructed a CTF (coarse-to-fine) model detection approach on the basis of OF (optical flow) and stable metrics. OFsum consistency was analyzed for discovering the suspicious tampered points. The forgery was detected at exact location such as duplicated frame pairs matching on the basis of OF correlation and authentication checks for further mitigating the FD (false detection). Three publicly available datasets of videos executed in the experimentation. The results demonstrated that the devised technique detected the unsmooth manipulation and common smooth forgery effectively and accurately and performed vigorously against the regular attacks namely additive noise, filtering, and compression.

Hosny [23] presented a CNN (convolutional neural network) model in order to detect forgery in CM (copy-move) image. This model became lightweight due to the appropriate number of convolution and max-pooling layers. A testing was done quickly and precisely at 0.83 seconds. The presented model was quantified on the benchmark datasets in the experimentation in which accuracy and time was considered as metrics. The experimental results depicted that the accuracy of the presented model was calculated 100%.

Murugan [24] intended an effectual technique to detect forgery in copy-move and locate the tampered regions. For this, the SIFT key-points were clustered and relative neighbourhoods were considered. This technique was implemented to aggregate and match the key-points into several small clusters concerning scale and color. Consequently, the temporal complexity launched with SIFT (scale-invariant feature transform) was lessened. A unique localization technique method was put forward for analyzing the comparable neighbours of matched pairs in accordance with 2 similarity indices. Afterward, pixel-level tampered areas were discovered by assigning the labels to the tampered regions into pixels. Image processing assisted in manipulating the digital images. In the experimental outcomes, the intended technique was proved applicable to localize the forgery and reliable to detect the forgery in comparison with other methods.

Ashraf [25] designed a method to detect the forgery in copy-move in which Discrete Wavelet Transform (DWT) algorithm was utilized. This algorithm had potential for analyzing the image contents on edges or to abrupt the changes in color contrast. This algorithm was capable of decomposing the image into four sub-bands. The implementation of this method was done on the basis of approximation sub-band for diminishing the size of the image that led to lessen the execution time. The experiment outcomes indicated the adaptability of the designed method to detect and localize the copy-moved region. Thus, this method was helpful in diverse fields including the judiciary, media and crime investigation.

Zhou and Tian *et al.* [26] became the first to introduce an image copy-move forgery passive detection method by combining the improved Pulse Coupled Neural Network (PCNN) and the self-selected sub-images. The dual feature matching is used to match the features and locate the forgery regions. The self-selected sub-images can quickly obtain suspected forgery sub-images and lessen the workload of feature extraction and achieved invariance of rotation, scaling, noise adding and the improved PCNN can extract image features with high robustness. Through experiments on the standard image forgery datasets CoMoFoD and CASIA, it was effectively verified that the robustness score and accuracy of proposed method was much higher.

Dixit and Bag [27] worked on a technique technique to detect copy-move image forgery with reflection and non-affine transformation attacks. The detection technique was based on Center Surround Extrema (CenSurE) detector. To compute keypoint descriptors, Local Image Permutation Interval Descriptor (LIPID) is used. Keypoint matching is performed using k-Nearest Neighbor (k-NN) technique with utilization of k-d tree and Best-Bin-First (BBF) search method. The approach also shows robustness against erosion, dilation, RGB color addition, zoom motion blur, JPEG compression, spread noise addition, and multiple copy-move attacks. Proposed scheme consumes least time in forgery detection as compared to state-of-the-art methods.

Krishnaraj *et al.* [28] worked on an automated deep learning-based fusion model for detecting and localizing Copy-Move Forgeries (DLFM-CMDFC). The proposed technique combines models of generative adversarial networks (GANs) and densely connected networks (DenseNets). The two outputs are combined in the DLFM-CMDFC technique to create a layer for encoding the input vectors with the initial layer of an extreme learning machine (ELM) classifier. Additionally, the ELM model's weight and bias values are optimally adjusted using the artificial fish swarm algorithm (AFSA). The networks' outputs are supplied into the merger unit as input. Finally, a faked image is used to identify the difference between the input and target areas. Two benchmark datasets are used to validate the proposed model's performance. The experimental results established the proposed model's superiority over recently developed approaches.

Ali *et al.* (2022) [29] introduced robust deep learning-based system for identifying image forgeries in the context of double image compression. The difference between an image's original and recompressed versions is used to train our model. The proposed technique explores numerous artifacts left behind in the image tampering process, and it takes advantage of differences in image sources through image recompression. This technique can detect both image splicing and copy-move forgeries. The proposed model is lightweight, and its performance demonstrates that it is faster than state-of-the-art approaches.

III. GLCM and BRISK

GLCM stands for Gray Level Co-occurrence Matrix works on the concept of frequency of gray levels of the image occurring in a unit area. This function measures the value of occurrence of pixel value with entropy, energy, dissimilarity among many other features in a certain spatial association to a pixel of a certain value. Although the algorithm has been used before however the method has not been used along with the BRISK algorithm. Due to the usage of a matrix-based function, the algorithm is able to cover almost all the pixels in an image to calculate the intensity of different factors in much short span of time than (CHT) Circular Harmonic Transformation technique used in existing method.

BRISK is one of the top three algorithms known for its rotation and scaling invariance. For one or another reason, if GLCM is unable to read or extracts the features of an image for invariance, BRISK will help to process such images. It is a feature point detection algorithm with lower computational cost as compared with CHT (circular harmonic transformation) technique used in existing method. BRISK achieves the invariance implementing the measure orientation of the keypoint and rotating the pattern by that orientation. First it is applied to bigger pairs of pixels and then smaller pairs. Such segregation helps in achieving maximum accuracy and execution speed.

IV. Research Methodology

The research methodology is the main component of any research. It clearly shows the working of the whole process. A brief task of each step is also mentioned at every step.

The proposed technique can be pictorially seen in the Fig. 3. The step-by-step process is briefly given below.

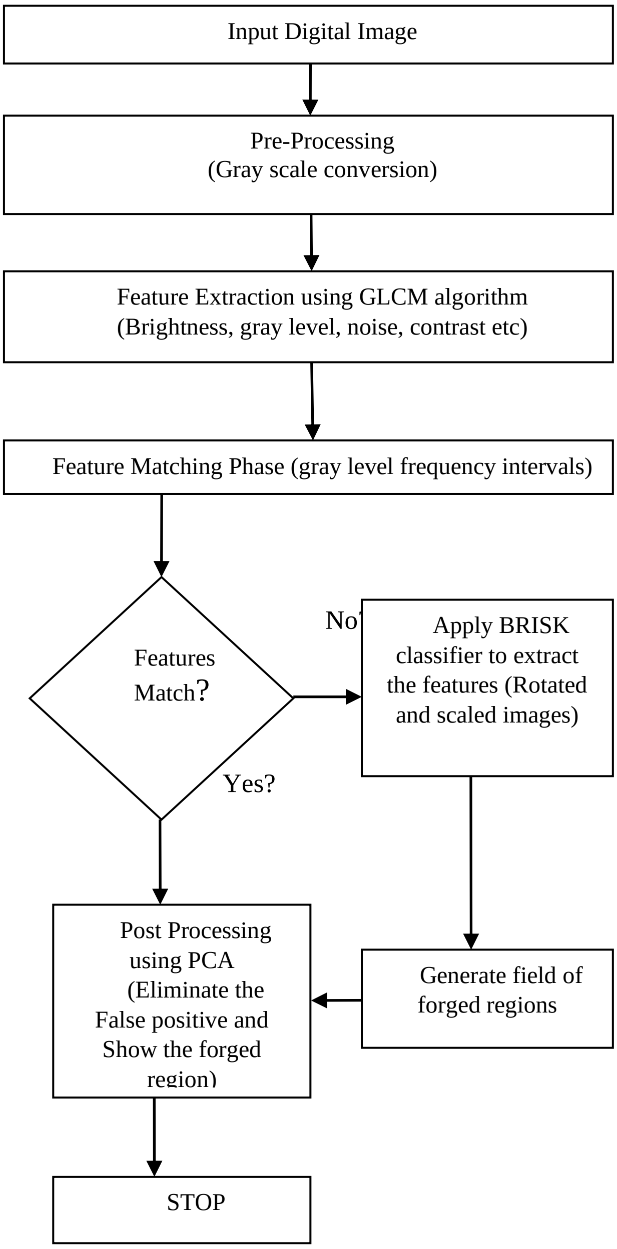
Input Digital Image
Pre-Processing
(Gray scale conversion)
Feature Extraction using GLCM algorithm
(Brightness, gray level, noise, contrast etc)
Feature Matching Phase (gray level frequency intervals)
Features
Match?
No
Apply BRISK classifier to extract the features (Rotated and scaled images)
Yes?
Post Processing using PCA (Eliminate the False positive and Show the forged region)
Generate field of forged regions
STOP

Figure 3. Research Methodology Flowchart

Input Digital Image: Like every other detection technique, first step is of loading image from a dataset. The images are taken from CoMoFoD dataset of 1200 forged and processed images. This dataset comprises images of various formats.

This research is carried out on number of images out of which, only one sample image is presented to avoid the complexity of the manuscript which is shown in Fig. 4. The initial data is a colored (RGB) image, in the next step this picture is further transformed into gray scale representation in order to precede further image processing operations.

Pre-Processing: It is the preliminary step in which the image is converted into grayscale and is then converted, transformed or decomposed. This step converts RGB pixels in grayscale image with a spectrum of 0−255. The main features and properties of the image such as brightness, color contrast, entropy is analysed in this phase. The image after the pre-processing phase as shown in Fig. 5 is ready to for extraction of features. This phase also eliminates noise levels from the image if any.

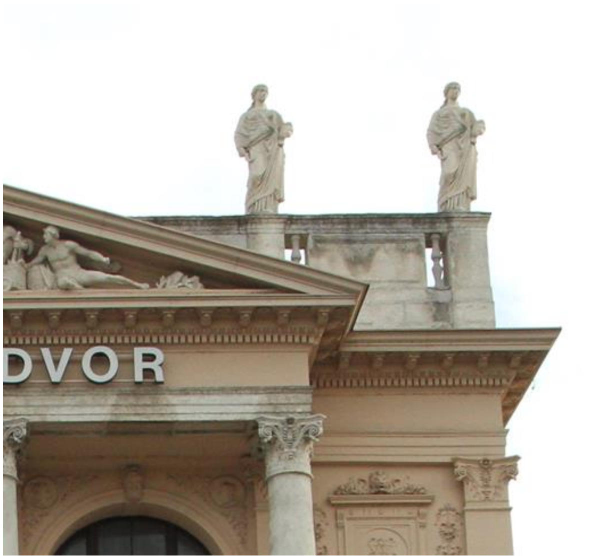

Figure 4. Manipulated image.

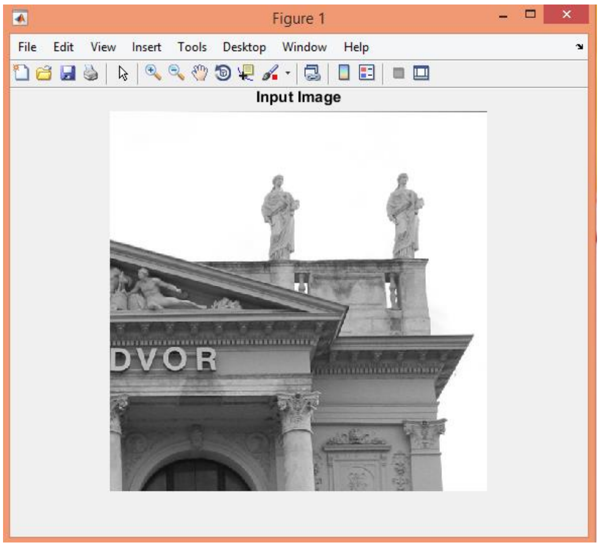

Figure 5. Grayscale conversion.

Feature Extraction: In this research work, the features such as correlation (joint probability occurrence of the specified pixel pairs), energy (sum of squared elements), contrast (local variations), dissimilarity and homogeneity are extracted using GLCM algorithm by matching grayscale levels and their occurring frequency (GLCM calculates in what a way a pixel with intensity i occur horizontally, vertically or diagonally to a pixel with intensity j). A matrix which comprises equal number of rows, columns and gray levels in an image is called GLCM. The highest matching keypoints will be recorded and matched. Provided that GLCM algorithm contains information about texture features for which it will be easy to carry out the extraction process. The texture features are calculated at particular positions corresponding to each other using statistical texture analysis. On the basis of available intensity points within each combination, the statistics is classified in first-order, second-order and higher order. The second order statistical texture features can be extracted easily with the help of GLCM algorithm. The GLCM algorithm provides information related to the positions of pixels that include similar gray level values.

Pseudo Code of GLCM Algorithm

```
1. In the matrix all the number of pixels is counted
   at which data is saved.
2. In matrix P[i,j], store the counted pixels.
3. Deploy histogram method for checking the
   similarity between pixels in the matrix.
4. Calculate contrast factor from the matrix.
5. The pixels are divided to fulfil the demands of
   normalizing the elements of g.
6. $g = \begin{bmatrix} 0.8\ if g < 0.8 \\ 1.2\ if g > 1.2 \\ g otherwise \end{bmatrix}$

   $g = \exp\left[\frac{mean(I) - minimum(I)}{maximum(I) - mean(I)}\right].$
```

Further, a special as well as an effective technique by the name of Binary Robust Invariant Scalable Keypoints (BRISK) has been used to detect the forgeries using multiscale corner features in a 2-D grayscale input digital image. The special thing about BRISK is that it is invariant to rotation and scaling factors. It will utilize the grayscale combination extract points inside the image and match them using Binary Feature descriptors. Along with this, two additional advantages of BRISK are its low storage memory and faster response time. It is denoted by a command line function:

```
points = detectBRISKFeatures(I);
```

Features matching phase: The matching of keypoints which are extracted from the input image is done with each other for the recognition of same points inside the image. The identical regions are discovered in an image using the value of threshold in the presented forgery detection techniques. The value of threshold is chosen heuristically. But the blocks made with the help of GLCM output are known to be the most appropriate features of the image so we can say the threshold value we achieved must have the best value above which, we can say that the pixel doesn't have any kind of informatics value of the feature of the image, so we can discard that pixel. Similarity matching is performed within the pixels, once the required pixels are obtained. The pixels of the blocks which are dissimilar will be detected as the forgery pixels.

Generate Forged regions: Once the feature matching phase completes, a field region of forged area is created which may have unrequited area also. It is a crucial phase for a forged image as it depicts the manipulation of an image in certain areas. The only position of forgery areas is the matching attribute points. The extraction of these areas is performed in more accurate manner.

PCA algorithm: Now that a forged field is created along with some unrequited areas which may or may not have forged regions, PCA algorithm will eliminate the unwanted areas from the image and will show us the forged regions clearly. The copied region is marked with black color with the help of PCA algorithm, it is a multivariate manner which is used to analyse data table generated in the background. This data table represents several interrelated quantitatively dependent variables. The major purpose of this approach is the extraction of important information from the table for the representation of novel orthogonal variables. These variables are known as principal components. The patterns of similarity of observations and the variables in the form of points within maps are displayed here. The data is centred primarily with respect to each variable when a given data matrix contains p variables and n samples. On the origin of principal components, the data occurs in the middle which however does not influence the spatial relations of data or the variances present along the variables. The initial principal component (Y_1) is specified through the linear combination of variables (denoted with X) as X_1, X_2, ..., X_p which is given below:

$$Y_1 = a_{11}X_1 + a_{12}X_2 + \cdots + a_{1p}X_p \quad (1)$$

In the form of matrix notation, it can be specified as:

$$Y_1 = a_1^T X \quad (2)$$

The initial principal component is calculated for finding the greatest possible variance within the data set. Selecting large values for weights $a_{11}, a_{12}, \dots a_{1p}$, the variance of Y_1 can be made. The weights are computed with the constraint such that the sum of squares is 1, to prevent such condition.

$$a_{11}^2 + a_{12}^2 + \cdots + a_{1p}^2 = 1 \quad (3)$$

The second principal component is computed in same way as no correlation occurs towards the initial principal component. The next highest variance utilizes this second principal component.

$$Y_2 = a_{21}X_1 + a_{22}X_2 + \cdots + a_{2p}X_p \quad (4)$$

This process is repeated till the computation of p principal components. These components are equal to the original number of variables. Equivalent values are obtained for the sum of variances of all principal components and the sum of variances of all variables in this point. Therefore, the alterations of all original variables to the principal components can be demonstrated as:

$$Y = XA \quad (5)$$

The principle components of the image which are the forged regions are highlighted and marked with black color through PCA algorithm as depicted in Fig. 6.

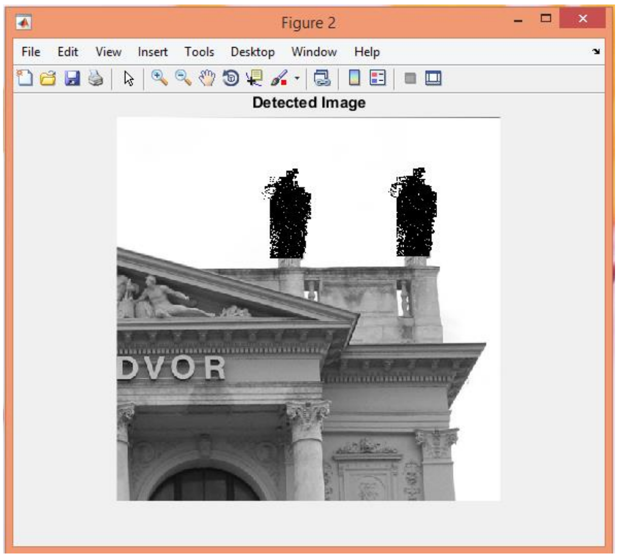

Figure 6. Mismatched regions.

IV. Results and Discussions

This research work is evaluated on CoMoFoD dataset on the following parameters at image level as well as pixel level as shown in Table I. The results are obtained implementing the research work in MATLAB R2015 a v8.5.0.197613

a. Precision: In pattern recognition, information retrieval and binary classification, precision (also called positive predictive value) is the fraction of relevant instances among the retrieved instances.

$$Precision = \frac{TP}{TP + FP}$$

b. Recall Rate: Recall is the fraction of relevant instances that have been retrieved over the total amount of relevant instances.

$$Recall = \frac{TP}{TP + FN}$$

c. F-Measure: It is calculated as the harmonic mean of precision and recall, giving each the same weighting. It allows a model to be evaluated taking both the precision and recall into account using a single score, which is helpful when describing the performance of the model and in comparing models

$$F - score = \frac{TP}{TP + 1/2(FN + FP)}$$

TABLE I. Results after Feature Matching Phase

Level	Precision	Recall	F-Measure
Image Level	0.98	0.98	93.54
Pixel Level	0.98	0.98	95.16

This research work also does the quantitative analysis on brightness changes on images and the results are shown in Table II.

TABLE II. Quantitative Results for Brightness Changes

Parameters	Proposed Technique
Precision	0.98
Recall	0.98
F1 measure	91.93

V. Conclusion

The copy-move forgery detection is the technique which is applied to detect forged portion from the image. Image processing is used to process data accumulated as picture elements. The tampered region of input pictures can be detected with the help of forgery detection approach. GLCM algorithm is implemented in conjunction with BRISK algorithm in this research work to detect forgery. In GLCM algorithm, the textural properties of picture are identified by computing co-occurrence matrix. The GLCM technique is described with PCA methodology which removes the false positives within the image

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Amarpreet Singh guided Sanjogdeep Singh to carry out this research work. Sanjogdeep found the relevant material and researched the knowledge material from various listed sources. Both the authors discussed the topic content and designed the flowchart. The finishing touches for the manuscript were done by Sanjogdeep Singh.

References

[1] T. Zhu, J. Zheng, Y. Lai, *et al.*, "Image blind detection based on LBP reside classes and color regions," *PLoS ONE*, 2019.

[2] N. Kanwal, A. Girdhar, L. Kaur, *et al.*, "Detection of digital image forgery using fast Fourier transform and local features," in *Proc. International Conference on Automation, Computational and Technology Management*, 2019.

[3] H. Kasban and S. Nassar, "An efficient approach for forgery detection in digital images using Hilbert-Huang transform," *Applied Soft Computing*, 2020.

[4] Y. William, S. Safwat, and M. A. M. Salem, "Robust image forgery detection using point feature analysis," in *Proc. Federated Conference on Computer Science and Information Systems (FedCSIS)*, 2019.

[5] N. S. Monson and K. V. M. Kumar, "Behaviour knowledge space-based fusion for image forgery detection," in *Proc. International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2017.

[6] K. Hayat and T. Qazi, "Forgery detection in digital images via discrete wavelet and discrete cosine transforms," *Computers & Electrical Engineering*, 2017.

[7] G. Ramu and S. B. G. T. Babu, "Image forgery detection for high resolution images using SIFT and RANSAC algorithm," in *Proc. 2nd International Conference on Communication and Electronics Systems (ICCES)*, 2017.

[8] A. Baumy, M. Abdalla, N. F. Soiliman, *et al.*, "Efficient implementation of pre-processing techniques for image forgery detection," in *Proc. Japan-Africa Conference on Electronics, Communications and Computers (JAC-ECC)*, 2017.

[9] N. Huang, J. He, and N. Zhu, "A novel method for detecting image forgery based on convolutional neural network," in *Proc. 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications / 12th IEEE*

International Conference on Big Data Science and Engineering (TrustCom/ BigDataSE), 2018.

[10] G. Nirmala and K. K. Thyagharajan, "A modern approach for image forgery detection using BRICH clustering based on normalised mean and standard deviation," in *Proc. International Conference on Communication and Signal Processing (ICCSP)*, 2019.

[11] Y. Wei, X. Bi, and B. Xiao, "C2R net: The coarse to refined network for image forgery detection," in *Proc. 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications / 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/ BigDataSE)*, 2018.

[12] G. Muzaffer, G. Ulutaş, and E. Gedikli, "PSO and SURF based digital image forgery detection," in *Proc. International Conference on Computer Science and Engineering (UBMK)*, 2017.

[13] H. A. Alberry, A. A. Hegazy, and G. I. Salama, "A fast SIFT based method for copy move forgery detection," *Future Computing and Informatics Journal*, 2018.

[14] G. Muzaffer, G. Ulutas, and B. Ustubioglu, "Copy move forgery detection with quadtree decomposition segmentation," in *Proc. 43rd International Conference on Telecommunications and Signal Processing (TSP)*, 2020, pp. 208–211.

[15] Y. Liu, C. Xia, X. Zhu, *et al.*, "Two-stage copy-move forgery detection with self deep matching and proposal SuperGlue," *IEEE Transactions on Image Processing*, vol. 31, pp. 541–555, 2022.

[16] R. Thakur and R. Rohilla, "Copy-move forgery detection using residuals and convolutional neural network framework: A novel approach," in *Proc. 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC)*, 2019, pp 561−564.

[17] Z. Hossein-Nejad and M. Nasri, "Adaptive stopping criteria-basec A-RANSAC algorithm in copy move image forgery detection," ir *Proc. 12th International Conference on Information anc Knowledge Technology (IKT)*, 2021, pp. 107–111.

[18] Y. Gan and J. Yang, "An effective scheme for copy-move forger detection using polar sine transform," in *Proc. 2nd Internationa Conference on Safety Produce Informatization (IICSPI)*, 2019, pp 337−341.

[19] J. Zheng and K. Zhang, "Copy-Move forgery detection algorithn based on feature point clustering," in *Proc. IEEE 6th Informatior Technology and Mechatronics Engineering Conference (ITOEC)* 2022, pp. 775–780.

[20] Y. Li and J. Zhou, "Fast and effective image copy-move forger detection via hierarchical feature point matching," *IEEI Transactions on Information Forensics and Security*, vol. 14, no 5, pp. 1307–1322, May 2019.

[21] W. Zhang and X. Tang, "Copy move forgery detection based or dense-field and sparse-field method," in *Proc. IEEE Intl Conf or Dependable, Autonomic and Secure Computing, Intl Conf or Pervasive Intelligence and Computing, Intl Conf on Cloud anc Big Data Computing, Intl Conf on Cyber Science and Technolog Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 2021, pp 500–506.

[22] S. Jia, Z. Xu, H. Wang, *et al.*, "Coarse-to-fine copy-move forgery detection for video forensics," *IEEE Access*, vol. 6, pp. 25323–25335, 2018.

[23] K. M. Hosny, A. M. Mortda, M. M. Fouda, *et al.*, "An efficient CNN model to detect copy-move image forgery," *IEEE Access*, vol. 10, pp. 48622–48632, 2022.

[24] A. Murugan, M. Arsath A, M. Anandaraj, *et al.*, "Similar neighbourhood search and key-point clustering in forgery detection," in *Proc. International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2022, pp. 1375–1380.

[25] R. Ashraf, M. S. Mehmood, T. Mahmood, *et al.*, "An efficient forensic approach for copy-move forgery detection via discrete wavelet transform," in *Proc. International Conference on Cyber Warfare and Security (ICCWS)*, 2022, pp. 1–6.

[26] G. Zhou, X. Tian, and A. Zhou, "Image copy-move forgery passive detection based on improved PCNN and self-selected sub-images," *Frontiers of Computer Science*, vol. 16, no. 4, pp. 1–16, 2022.

[27] A. Dixit and S. Bag, "A fast technique to detect copy-move image forgery with reflection and non-affine transformation attacks," *Expert Systems with Applications*, vol. 182, 115282, 2021.

[28] N. Krishnaraj, B. Sivakumar, R. Kuppusamy, *et al.*, "Design of automated deep learning-based fusion model for copy-move image forgery detection," *Computational Intelligence and Neuroscience*, 8501738, 2022.

[29] S. S. Ali, I. I. Ganapathi, N. S. Vu, *et al.*, "Image forgery detection using deep learning by recompressing images," *Electronics*, vol. 11, 403, 2022. https://doi.org/10.3390/electronics11030403

Amarpreet Singh has completed his PhD. Currently he is working as a professor in Amritsar Group of Colleges Amritsar, Punjab, India. He has published number of research papers in various international/ national journals and conferences. His area of interest is Network security and digital image processing.

Sanjogdeep Singh has completed bachelor's of Technology in CSE degree from Punjab Technical University. Currently he is studying master's of Technology. His area of interest is digital image processing.