Image Forgery Detection Using Noise and Edge Weighted Local Texture Features

Khurshid ASGHAR[1], Mubbashar SADDIQUE[2,3], Muhammad HUSSAIN[4], George BEBIS[5], Zulfiqar HABIB[6]
[1,2,6]*Department of Computer Science, COMSATS University Islamabad, Pakistan*
[3]*Department of Computer Science & Engineering, University of Engineering & Technology Lahore (Narowal Campus), Pakistan*
[4]*Department of Computer Science, King Saud University, Riyadh, Saudi Arabia*
[5]*Department of Computer Science and Engineering, University of Nevada, at Reno, USA*
drzhabib@cuilahore.edu.pk

***Abstract*—Image forgery detection is important for sensitive domains such as courts of law. The main challenge is to develop a robust model that is sensitive to tampering traces. Existing techniques perform well on a limited dataset but do not generalize well across the datasets. Moreover, these techniques cannot reliably detect tampering that distorts the texture pattern of the image. The noise patterns remain consistent throughout a digital image if its contents are not altered. Based on this hypothesis, a robust descriptor FFT-DRLBP (Fast Fourier Transformation - Discriminative Robust Local Binary Patterns) is introduced, which first estimates noise patterns using FFT and encodes the discrepancies in noise patterns using DRLBP. Features extracted are passed to Support Vector Machine (SVM) for deciding whether the image is authentic or tampered. Intensive experiments are performed on benchmark datasets to validate the performance of the method. It achieved an accuracy of 99.21% on the combination of two challenging datasets. The comparison shows that it outperforms state-of-the-art methods and is vigorous to image forgery attacks even in the presence of various post-processing operations. The performance of the method is also validated using cross-dataset experiments, which ensures its robustness and generalization.**

***Index Terms*—artificial intelligence, forgery, Fourier transforms, machine learning, pattern recognition.**

I. INTRODUCTION

Digital images have applications in almost every field of life, such as the World Wide Web, electronic and print media, the insurance industry, forensic science, court of law and security, etc. Due to easy access to high-resolution digital cameras and powerful image editing software, images can be captured and manipulated (forged) to gain illegal advantages such as false propaganda, fraud, counterfeiting, and blackmailing. Therefore, it is necessary to ensure the authenticity of the images.

Active techniques, such as digital watermarking, are effective in verifying the authenticity of an image, but the requirement of embedding a watermark into an image limits their widespread use in practice. The alternative approach is passive image forgery detection, which does not require embedding any watermark or signature. A device signature is embedded in the form of noise patterns at the time of capturing; image tampering operations disturb these noise patterns [1]. It follows that for forgery detection, noise patterns can be considered as an intrinsic watermark embedded in an image of the source device. In view of this, many image forgery detection methods have been proposed, which are based on noise estimation. These techniques estimate noise patterns using different de-noising algorithms [2-3], such as noise estimation by Principal Component Analysis (PCA) [4] and noise estimation by multi-scale image segmentation [5]. The noise estimation methods, which have been employed in these techniques, are designed keeping in view a specific type of noise. Usually, the type of noise is not known to tackle this problem; different methods are simultaneously used to estimate noise patterns and represent an image for forgery detection [6-10]. For coding, most of the methods use statistical measures such as mean, standard deviation, etc. Noise estimation is the main challenge to develop a successful image forgery detection system. We propose a simple technique for noise estimation, which does not consider the type of noise and is effective for forgery detection. Also, we propose to use a robust technique for coding, which encodes the distribution of discriminating noise patterns. Based on the proposed descriptor for noise estimation and its coding, we introduce a new technique to authenticate whether an image is forged or not.

Noise is a high-frequency content of an image. Based on this fact, instead of using de-noising algorithms [11], we have estimated noise patterns using a generic approach based on Fast Fourier Transform (FFT) and high-pass filtering [12]. For implementation, we have employed Discriminative Robust Local Binary Patterns (DRLBP) [13], which encodes the discrepancies in noise patterns. We call the FFT-DRLBP based descriptor, which represents an image and is used for verifying its authenticity. Finally, FFT-DRLBP descriptor and Support Vector Machine (SVM) are used to predict whether an image is authentic or forged.

This paper has following contributions: (i) Any type of noise has been utilized for detection of forgery. (ii) A new descriptor named FFT-DRLBP has been introduced. (iii) The parameters of SVM are tuned to classify a given image as authentic or forged. (iv) Good accuracy is achieved through cross dataset validation as well. The results indicate that the proposed method outperforms state-of-the-art methods.

The remainder of the paper is organized as follows:

The research was supported under Researchers Supporting Project number (RSP-2019/109) King Saud University, Riyadh, Saudi Arabia.

Digital Object Identifier 10.4316/AECE.2022.01007

Previous works on image forgery detection are reviewed in Section II. The detail of the proposed technique is described in Section III. Section IV explains FFT-DRLBP descriptor. Experimental setup is described in Section V. Experimental results are presented and discussed in Section VI. Comparisons with existing works are performed in Section VII. The cross-dataset results are presented in Section VIII. The paper concludes in Section IX.

II. Related Work

Most of the existing image forgery detection methods are block-based or key-point-based [14]. Alfy et al., [15] exposed image tampering using Local Binary Pattern (LBP), DCT, and Markov moments. Their method achieved good results on CASIA v2.0 dataset. Luo et al., [16] extracted color moments from red, blue, and green channels to expose image forgery . This method was robust only against blurring. They used Singular Value Decomposition (SVD) and proved the robustness of their method against forged images distorted by noise. Fourier Mellin Transform (FMT) together with the 1D projection of log-polar values to detect image forgery was applied by Bayram et al., in [17]. Mahdian et al., in [18], used blur invariant moments to detect a forgery in the presence of blurring and contrast enhancement. Wu et al., used Dual-Tree Complex Wavelet transform (DT-CWT) to detect image forgeries [19].

To remove noise in images is an important aspect in the field of image processing. Noise is used as a tampering cue in recent research methods [1], [20-21]. Popescu et al., [22] represented image features by measuring the noise variance using statistical tools such as mean and standard deviation. A blind signal-to-noise ratio (SNR) estimator was developed to measure this noise variance across the image as evidence of tampering. The idea behind this approach is that if two images are spliced together, or if a small amount of noise is locally added to conceal traces of tampering, then noise patterns become inconsistent. This method was used to localize the forgery and tested on a very small number of images. Guo et al., [23] developed a set of statistical features based on extracting noise using de-noising filters, wavelet analysis, and neighborhood prediction. This method achieved 90% accuracy with a 5% false-positive rate. The technique was not robust against JPEG compression. Mahdian et al., [24] in , represented noise patterns using the high pass wavelet coefficients. The method was designed to localize the forgery. No benchmark dataset was used for evaluation estimated noise using wavelet and DCT to detect a forgery in the image. The method is dependent on the kurtosis property of the source image. Kang et al., [25] developed an image authentication method based on sensor patterns, but it depends on sensor noise and is not robust to high JPEG compression.

Stamm et al., in [26], proposed a method based on statistical intrinsic noise patterns. This work detects forgery by means of contrast enhancement; however, the performance is not quantitatively measured. Fan et al., [3] estimated Exchangeable Image File Format (EXIF) parameters such as aperture, shutter speed, and ISO speed rating based on noise features for image manipulation detection. This method was evaluated on specific camera models. Ke et al., in [4], estimated noise variance using PCA to detect a forgery in images. Their method detected blurred inconsistencies in images effectively. Detection performance is not mentioned quantitatively. Liu et al., in [27], estimated noise using Gaussian de-noising filters to authenticate images. Their method has low accuracy at high JPEG compression. Chierchia et al., in [28], developed the Bayesian MRF approach in which Photo Response Non-Uniformity (PRNU) is measured to Bayesian Markov Random Fields (MRF) approaches. Their method provides consistent performance in terms of detecting object-level forgery. Their method is not good to detect small object-level forgery. Yang et al., in [29], proposed an image forgery detection method based on multi-granularity superpixels matching. This method performed well but was not robust to strong image manipulation operations. Wang et al., in [30] proposed mass filter banks using fast Fourier transformation. The features were then fed to ResNet [31] to classify whether an image is tampered with or authentic. During the process of image tampering, structural changes can be made easily due to the strong tools available, and it becomes very difficult to know which part of the image is tampered with. Vinod Mall et al., [32] used a hash function to expose the structural changes to detect the image forgery.

Different classifiers have been exercised in the literature for different applications in the various fields of life. For example SVM classifier has been used in the medical applications [33], crop disease classification. Similarly, CNN has been implemented for different applications [34, 35]. However, the CNN has one of the limitations that it requires a GPU based system for the training purposed. Fuzzy models have been utilized for the classification [36-37].

A review of existing image forgery detection techniques shows that the detection of structural changes, splicing, and copy-move forgery is still a challenge. In this paper, we propose a new method to authenticate images based on the estimation of noise without prior knowledge of noise type. The proposed framework is simple, generic, and capable of modeling structural changes that occurred in images due to forgery.

III. Proposed Scheme

To develop a robust non-intrusive method of image forgery detection, it is useful to model the intrinsic characteristics of a tampered image because any image-altering operation disturbs its intrinsic properties [38]. Noise is an intrinsic characteristic of an image that has a uniform distribution if the image is not altered. A tampering operation such as copy-move or splicing distorts the noise patterns of an image. Some image forgery detection methods [2], [24], [27], [39], [40] are based on this assumption, i.e., noise patterns have been analyzed for forgery detection. The proposed method is also based on this assumption. The key question is how to analyze noise patterns? Addressing this question, we propose a simple and robust descriptor, called the FFT-DRLBP descriptor, which first estimates noise patterns using Fast Fourier Transform (FFT) and then encodes the noise distribution using DRLBP texture descriptor. This descriptor has already been used for image and video forgery detection [41-42]. The proposed descriptor does not consider the type of noise in an image,

which is usually not known; as such, it is widely applicable. The features extracted through FFT-DRLBP descriptor from an image is passed to SVM for training the model which takes the decision whether the given image is authentic or forged.

The proposed approach is summarized into two phases: training (development of image forgery detection model) and testing (detection of unseen images). The training phase involves learning the structural changes that occurred in images due to forgery and what makes the forged images different from authentic images. The testing phase consists of using learned knowledge in an automatic way for testing unknown images. The proposed scheme is shown in Figure 1.

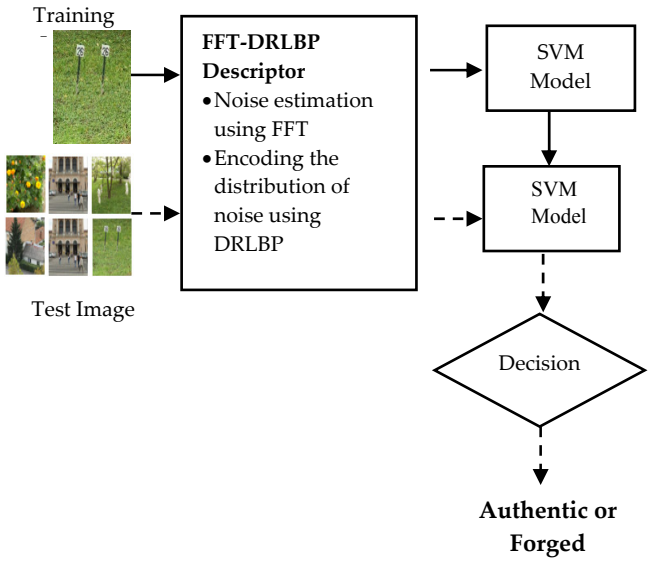


Figure 1. Flow diagram of FFT-DRLBP based proposed approach

A. *FFT-DRLBP Descriptor*

Noise is an intrinsic characteristic of an image, and its distribution is uniform if the image is not tampered. When image regions from the same image (copy-move) or other images (splicing) are pasted, and post-processing operations such as JPEG compression, blurring, or contrast enhancement are performed to conceal tampering, the noise patterns of the image become inconsistent. Based on this assumption, the problem of forgery detection is defined in the following way: If the distribution of noise in each image is uniform, the image is authentic; otherwise, it is tampered. This means that to detect image forgery, and there is a need to address two questions: (i) how to estimate noise? and (ii) how to encode noise?

TABLE I. SNR VALUES CORRESPONDING TO GHF AND BHF WITH DIFFERENT D_0

D_0	SNR (dB)	
	GHF	BHF
200	0.5626	0.4168
230	0.4717	0.3212
260	0.2985	0.2791
280	0.3526	0.2145
300	0.2858	0.2458

Addressing these two questions, we propose an FFT-DRLBP descriptor (see Figure 2) that first estimates noise patterns using FFT and then encodes them using DRLBP. The effectiveness of the proposed FFT-DRLBP descriptor on image forgery detection is statistically shown in Section 4.4. Next, we describe how noise patterns are estimated and encoded to compute the FFT-DRLBP descriptor.

B. *Estimation of Noise Patterns*

In this section, we discuss the technique to estimate noise patterns of an image for tampering detection. For the FFT-DRLBP descriptor, image noise is estimated from each channel $Ch\{R,G,B\}$ of a given image I. Typically, image denoising algorithms are used to estimate noise patterns. For a given image I, its denoised version I_D is obtained by applying denoising operation. The estimated image noise n_I is then obtained by pixel wise subtraction as follows:

$$n_1(i,j) = I(i,j) - I_D(i,j) \tag{1}$$

Usually, denoising algorithms are designed keeping in view a specific type of noise, and as such, are not suitable for estimating noise patterns for forgery detection because the type of noise of an image whose authenticity is in question is not known. In view of this, instead of using a de-noising algorithm, our idea is to extract noise patterns using a generic approach based on FFT (see Figure 2a). Noise is a high-frequency content of an image. Using FFT [43], the image *f(x,y)* is represented in the frequency domain as *F(u,v)*. Using the filter transfer function *H(u,v)* of a high pass filter, *F(u,v)* is filtered to get *G(u,v)* so that it contains only high-frequency content, i.e., noise. Applying, Inverse Fast Fourier Transform (iFFT), *G(u,v)* is converted into noise image *g(x,y)* in the spatial domain. Two commonly used high-pass filters are Gaussian High Pass Filter (GHF) and Butterworth High Pass Filter (BHF). The filter transfer functions of GHF and BHF are defined by

$$GHF(u,v) = 1 - e^{\frac{-D^2(u,v)}{2D_0^2}} \tag{2}$$

$$BHF(u,v) = \frac{1}{1+\left[\frac{D_0}{D(u,v)}\right]^{2n}} \tag{3}$$

where, D_0 is the radius of the circle to cut off frequency, n is the order of the filter and $D(u,v)$ is the distance from the point (u,v) to the origin in frequency plane and is defined by

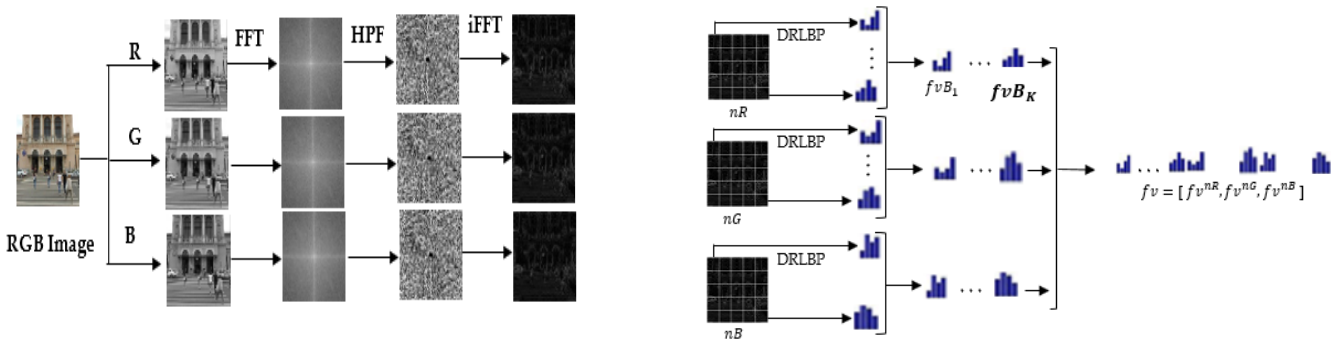
$$D(u,v) = \sqrt{(u-\frac{M}{2})^2 + (v-\frac{N}{2})^2} \tag{4}$$

The radius D_0 for cutoff frequency plays a vital role in keeping required detail. The experiments were performed with GHF and BHF filters using different values of D_0 to select the most appropriate value of D_0 on a combination of datasets (CASIA v1.0, CASIA v2.0 [44] and CoMFoD [45]). To select D_0, we employed the commonly used measure Signal to Noise Ratio (SNR), which measures the foreground signal strength relative to the background noise patterns. We adopted the following commonly used measure to compute SNR:

$$SNR = 10\log_{10}\left(\frac{P_{Signals}}{P_{Noise}}\right) \tag{5}$$

where, $P_{Signals}$ and P_{Noise} are estimated as the mean and standard deviation of the filtered image, respectively. The SNR values of the images filtered with GHF and BHF filters for different choices of D_0 are shown in Table I. As the smallest value of SNR indicates the better estimation of

noise and our purpose is to estimate noise, therefore we select BHF with D_0=280 because it results in the best estimate.



(a) (b)

Figure 2. Computation of FFT-DRLBP descriptor; (a) Noise patterns estimation, (b) Encoding the distribution of noise patterns using DRLBP

Algorithm 1: The computation of feature vector based on FFT-DRLBP

Input: RGB image I, the number of K Blocks
Output: FFT-DRLBP descriptor based feature vector Feature Vector (F.V)
Procedure:

1. Extract three channel of image I such that $Ch \in \{R, G, B\}$

2. For each $Ch \in \{R, G, B\}$ *do step 3 to 5*

3. Apply FFT on each channel Ch

4. Apply BHF with D_0=280 on each $\widehat{Ch}(u,v)$ *, where* $\widehat{Ch}$ *is FFT of Ch.*

5. Apply iFFT to get noise image nCh of channel Ch in spatial domain

6. For each channel $nCh \in \{nR, nG, nB\}$ *do Steps 1~6*

Step 1: For each pixel at location (x, y), compute weight $\omega_{x,y}$ *[13]*

$$w_{x,y} = \sqrt{I_x^2 + I_y^2}$$

where I_x and I_y are the first-order derivatives in the x and y direction.
Step 2: Compute image of LBP codes
Step 3: Compute weighted histogram H_{lbp} of LBP codes

$$H_{lbp}(j) = \sum_{x=0}^{L-1}\sum_{y=0}^{M-1} w_{x,y}\,\delta(LBP_{x,y}, j)\text{, where } j=1,2,\ldots,n$$

$$\delta(l.m) = \begin{cases} 1 & l = m \\ 0, & 0 \quad otherwise \end{cases}$$

where n is the number of LBP codes.
Step 4: Compute robust LBP (RLBP) histogram H_{rlbp} [30]
Step 5: Calculate difference LBP (DLBP) histogram H_{drlbp} [30]
Step 6: Compute DRLBP descriptor by concatenating RLBP and DLBP histograms and named this descriptor as FFT-DRLBP

7. Concatenate CH_{nCh}, $nCh \in \{nR, nG, nB\}$

8. F.V= concatenate $\{CH_{nR}, CH_{nG}, CH_{nB}\}$

C. Coding of Noise Patterns with FFT-DRLBP Descriptor

After estimating the noise image, the next step is to extract local noise patterns and estimate their distribution. Since the noise patterns of forged images are different from those of authentic images due to structural changes after forgery. As the noise patterns distorted near the boundary of forged areas in the forged image, the voted bin value is expected to be different for the forged image as compared to an authentic image which, in turn, helps in providing additional information (edges, lines) about tampered regions. The key question is how to model these noise patterns. To classify a given image as authentic or forged, noise patterns are required to be encoded with the strength of orientation and edge information. For this purpose, we adopt DRLBP descriptor because of its fast performance for computing complete structural information, which first encodes local changes in the form of LBP codes and then estimates their distribution considering the local gradient magnitude at the corresponding locations, i.e., DRLBP descriptor encodes the strength of noise patterns by encoding orientation and edge information together. Due to

the above mentioned reasons we combine this descriptor with the FFT and named it FFT-DRLBP descriptor. The following steps are followed to calculate the FFT-DRLBP descriptor.

(i) Gradient $\omega_{x,y}$ of every pixel of each channel $nCh \in \{nR, nG, nB\}$ is calculated using [13].

(ii) LBP image is calculated.

(iii) Weighted histogram H_{lbp} of LBP codes is also calculated.

(iv) The robust weighted histogram H_{rlbp} using [30] is computed to remove the reversal effects from the background and foreground.

(v) Discriminant weighted histogram H_{drlbp} is calculated to enhance the effects of pattern using [30].

(vi) DRLBP descriptor is computed by concatenating the H_{rlbp} and H_{drlbp} of each channel $nCh \in \{nR, nG, nB\}$. This descriptor is called FFT-DRLBP and its procedure is also explained in Figure 2 and Algorithm 1.

Algorithm 2: Training of image Forgery Detection Model

Input: F is the set of forged/tampered images, A is the set of authentic image, c (Regularized coefficient) and g (gamma) are the parameters of SVM with RBF kernel

Output: Trained classification model SVM

Procedure:

```
1   for each image in F,
        Create features vector (f.v) of each forged image using Algorithm 1
        (f.v)T =f.v
        Assigned label 1 to (f.v)T
    end for
2   for each image in A,
        Create features vector (f.v) of each authentic image using Algorithm 1
        (f.v)A =f.v
        Assigned label -1 to (f.v)A
    end for
3   D ← (f.v)_T ∪ (f.v)_A
4   AC=0
5   for c= min to max do
6       for g= min to max do
            Divide D into equally k folds (k=10)   % all training examples D
            for i=1 to k do
                Train SVM(c,g) on D-Fi to get SVMModel (c, g  % all training examples D except i^th fold Fi
                Test SVMModel (c, g) on fold Fi
                Record the AC(i) on fold Fi
            end for
            AvgAC = (1/k) Σ_{i=1}^{k} AC(i)        % compute average accuracy on k folds
            if ( AvgAC > AC)
            AC=AvgACC, cfiinal=c, gfinal=g
            end if
        end for
    end for
7   Fit the SVM (cfinal, gfinal) model on training data
```

D. SVM Based Classification Model

The identification of image as forged or authentic is a two-class problem and it is solved by train the model with SVM classifier, which has been selected due to its computational efficiency and robustness. The training of the model has been explained with Algorithm II. The SVM model takes the image as input and gives the decision whether the image is forged or authentic as shown in the Figure 1. The idea behind SVM is to select the hyper plane wit the maximum margin. However, the set of points that satisfy the minimum distance are the support vectors for the linear classifier but unfortunately, features are nonlinear and not separatable for higher dimension. In this case kernel trick is used to make the hyper plans linearly separatable. Different kernels have been proposed, however, in this paper RBF kernel has been selected empirically and tunned the parameters of this kernel to achieve good accuracy. The regularization coefficient c and g are tuned to $c=2^{-5}$ and $g=2^{-5}$ using grid search algorithm.

IV. Dataset and Evaluation Measures

In this section dataset description, evaluation measures, cross dataset evaluation, statistical analysis of the features and parameter tunning are explained in detail.

A. Datasets Description

The benchmark datasets CASIA v2.0 [44], CoMFoD [45], GRIP [46], Deutsche Welle Image Forensics (DWIF) [47], MICC-F220 [48], Image Manipulation (IMD) [49], Copy-Move Hard (CMH) [50], and Copy-Move Erlangen-Nuremberg (CMEN) [49], are used in the literature for evaluation of the algorithms. Therefore, in this study, we also performed experiments on these benchmark datasets for evaluating the proposed method. CASIA v2.0 dataset contains 7,491 authentic and 5,123 forged images. Images are in TIFF, JPEG, and BMP formats with resolutions varying from 240 × 160 to 900 × 600. CoMFoD dataset consists of 5,200 post-processed authentic and 5,200 post-processed forged images of resolution 512×512. Experiments were also performed by combining CASIA v1.0, CASIA v2.0 and CoMFoD datasets to evaluate the robustness of the proposed method in general. The combined dataset is named CASIA v1.0-CASIAv2.0-CoMFoD. GRIP dataset has 80 authentic and 80 forged PNG images of resolution 768×1024 pixels. DWIF dataset has 06 authentic and 12 forged JPEG images of 4896× 3264. MICC-F220 dataset has 111 authentic and 110 forged JPEG images of resolution 737 × 492. IMD has 48 authentic and 48 forged JPEG images of resolution 3888×2592. CMH dataset has 108 authentic images and 108 forged images, and the CMEN dataset has 363 authentic and 363 forged images. Both CMH and CMEN datasets have a variety of simple, rotated, and resized forgeries. UNISA [51] dataset contains 2000 authentic and 2000 tampered JPEG images with a variety of post-processing operations. IEEE Information Forensic Technical Committee Challenge (IEE IFS-TC) [52] contains 1050 authentic and 901 fake PNG images and 5713 test images. Wild Web Tampered Images (WWTI) [53] has 92 versions of 82 authentic images.

B. Performance Evaluation Measures

For evaluation, the forged images are considered as positive while the authentic as negative. The proposed method is evaluated using accuracy (ACC), true positive rate (TPR), false-positive rate (FPR), and area under the curve (AUC) [41] explained as follows.

1) Accuracy (ACC)

ACC is the percentage of correctly classified samples of the total number of classified images and is defined as

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \times 100\,\% \tag{6}$$

where, True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) are forged images correctively classified, authentic images correctively classified, authentic but classified as forged), and forged but classified as authentic, respectively.

2) True Positive Rate (TPR)

TPR or Sensitivity (*SN*) is the possibility of recognizing a forged image as forged and is computed by

$$TPR = SN = \frac{TP}{TP + FN} \times 100\,\% \tag{7}$$

3) True Negative Rate (TPR)

TNR or Specificity (*SP*) is the possibility of recognizing an authentic image as authentic which is calculated from

$$TNR = SP = \frac{TN}{TN + FP} \times 100\,\% \tag{8}$$

4) False Positive Rate (TPR)

The False Positive Rate (*FPR*) or specificity is the percentage of negative cases (i.e., authentic images) that are misclassified and is determined by

$$FPR = (1 - TNR) \times 100\,\% \tag{9}$$

5) Area Under the Curve (AUC)

ROC curve is used to envision the performance of the two-class classifier. It plots TPR versus FPR for exclusive thresholds of the classifier significance. Overall performance is represented by way of AUC values the following ways: excellent (0.9 -1.00), good (>= 0.80), fair (>= 0.70), poor (>= 0.60) and worthless (<= 0.50) [54].

C. Cross Dataset Evaluation

Cross dataset evaluation (training on one dataset and testing on another dataset) is the ultimate evaluation to expose the weaknesses of the trained model and make sure the robustness of any image forgery detection method. In our experimental analysis, the performance of the proposed image forgery detection system is also evaluated using a cross dataset. It is trained on a combination of CASIA v1.0, CASIA v2.0, and CoMFoD datasets and testing on datasets named DWIF, MICC-F220, IMD, CMH, CMEN, UINSA, IEE IFS-TC, and WWTI.

D. Statistical Analysis of FFT-DRLBP Descriptor

To show that the FFT-DRLBP descriptor has the potential to discriminate authentic and tampered images using image forgery, a statistical analysis of the descriptor is given in the following two different ways.

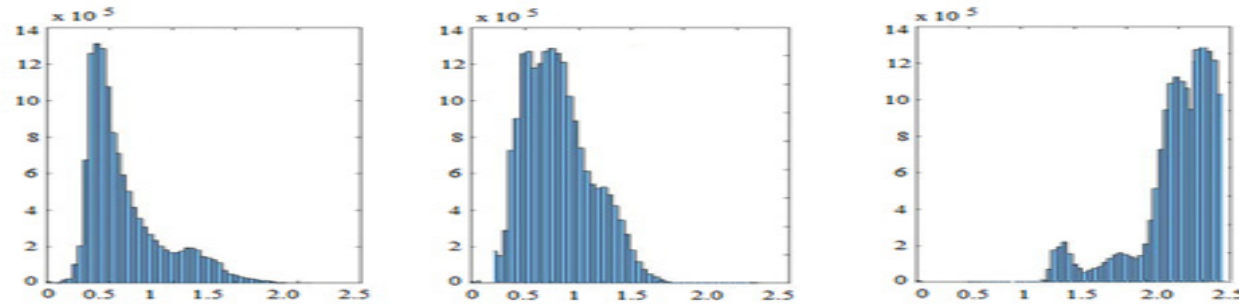
First, we computed the pairwise distances for the three cases using the city block [55] between (i) authentic images, (ii) forged images, and (iii) authentic and forged images using the dataset CoMFoD. The cases (i) and (ii) represent intra-class distances, whereas case (iii) represents inter-class distances; the histograms for the three cases are shown in Figure 3. Most of the pairwise distances for intra-class cases (see Figure 3a and Figure 3c) are between 0.0 and 1.5, while those for inter-class cases (see Figure 3b) are between 1.5 and 2.5. There is an overlap of approximately 4% between pairwise distances belonging to intra-class and inter-class cases. It indicates that the FFT-DRLBP descriptor has the potential of discriminating the authentic and forged images. The effect of the overlap is reduced when kernel SVM is used for classification because the kernel computes the distances in high dimensional feature space where the patterns are linearly separable.

Secondly, the effect of the DRLBP descriptor is analyzed using a scatter matrix-based measure because of its simplicity [56]. For this purpose, two scatter matrices: (i) within-class scatter matrix (*WS*) and (ii) between class scatter matrix (*BS*). *WS* and *BS* are defined by:

$$WS = \sum_{i=1}^{c} \sum_{j=1}^{N_i} (x_{ij} - \bar{x}_i)(x_{ij} - \bar{x}_i)^T \tag{10}$$

$$BS = \sum_{i=1}^{c} N_i (\bar{x}_i - \bar{x})(\bar{x}_i - \bar{x})^T \tag{11}$$

where, $\bar{x}_i = \frac{1}{N_i}\sum_{j=1}^{N_i} x_{ij}$ is the class mean and $\bar{x} = \frac{1}{N}\sum_{i=1}^{c}\sum_{j=1}^{N_i} x_{ij}$ is the overall mean of all classes for the given c sets of $N_i(1, 2,\ldots,c)$ vectors $x_{ij}(i=1,2,\ldots,c, j=1,2,\ldots,N_i)$ from c classes. T is the transpose of a matrix. The traces of *WS* and *BS* represent intra-class and inter-class scatters, respectively. The features are discriminative if the intra class scatter is small and inter-class scatter is high. Table II shows the traces of *WS* and *BS* for three data sets. In each case, the trace of „*BS* is high, whereas that of *BS* is small, indicating that the FFT-DRLBP descriptor is discriminative.



(a) (b) (c)

Figure 3. Pairwise distances of FFT-DRLBP features; within the authentic class (a), within the forged class (b), and between authentic and forged classes (c)

TABLE II. TRACE OF WS AND BS ON DRLBP FEATURES OF BENCHMARK DATASETS

Dataset	Trace of WS	Trace of BS
CASIA v2.0 [44]	1.37	2.57
CoMFoD [45]	1.48	2.21
IEE IFS-TC [52]	1.23	2.45

E. Parameter Tunning

The optimization of SVM parameters was done with the training datasets. The RBF kernel had the best performance. The RBF kernel involves two parameters: *c* (regularized coefficient) and *g* (gamma). The setting of these parameters plays a significant role in classification. The parameter *c* is used to balance the model complexity by fitting the minimum error rate. The kernel function parameter *g* is used to determine the nonlinear mapping from the input space to the high-dimensional feature space. Kernel parameters *c* and *g* were tuned to $c=2^{-5}$ and $g=2^{-5}$ using the grid-search method [57].

Moreover, the proposed system involves many parameters to estimate and encode noise patterns. Figure 4 illustrates the participating parameters. Tuning the parameters in a thorough manner to find the optimal set is not an easy task, which is considered an optimization problem. System parameters are tuned empirically (see Figure 4). To find the best parameters of the system, we performed a series of experiments. We have experimented with several thresholds of D_0 for both GHF and BHF and decided to use the BHF with $D_0=280$ to estimate noise patterns because it gave us the best experimental results (see Figure 4a). This is likely because the noise patterns obtained using the BHF filter [58] are encoded through DRLBP, and these encoded features are discriminative in nature. The statistical analysis of these features is also presented in Section 4.4. In the case of DRLBP, we found that the uniform (u2) LBP (maximum 2-bit transitions) with P=8 and R=1 is an appropriate choice due to its better performance (see Figure 4b and Figure 4c).

10-fold cross-validation is employed in which the forged and authentic images are randomly grouped into ten equal size folds. One-fold is held out in turn, and the remaining nine folds are used to train the model. The held-out folder is used to test the trained model; in this way, the model is trained and tested on different sets of images, i.e., the model is evaluated over different variations of the data. Ten performance measure values corresponding to the 10-folds are calculated, and their average is reported as the performance of the system. The same procedure is repeated for each dataset.

V. RESULTS AND DISCUSSION

Experimental results are presented in this section. First, we used a cross-validation protocol in which a given dataset is divided into ten-folds. The SVM parameters are tuned to the training images (nine out of the ten-folds), and that parameterization is used on the remaining (not used) fold for testing. This protocol is known as ten-fold cross-validation (CV); each time the testing fold changes, the parameters are recomputed on the appropriate training sets. Secondly, we used a cross-dataset validation protocol in which we trained on CASIA v1.0, CASIA v2.0, and CoMFoD datasets and tested on DWIF, MICC-F220, IMD, CMH, CMEN, UNISA, IEEE IFS-TC, and WWTI datasets. The SVM classifier is tuned on all images in the CASIA v1.0, CASIA v2.0, and CoMFoD datasets. Experimental results using 10-fold CV on different benchmark datasets are presented in Table III. The robustness of the method against different geometric transformations and different post-processing is discussed on different datasets in the next sub-sections.

TABLE III. EXPERIMENTAL RESULTS OF PROPOSED METHOD USING 10-FOLD CV ON BENCHMARK DATASETS

Datasets	ACC (%)	TPR (%)	FPR (%)	AUC
CASIA v2.0 [44]	99.54	99.82	0.39	0.99
CoMFoD [59]	99.13	98.67	0.99	0.99
GRIP [46]	97.00	98.11	2.47	0.98
CMH [50]	98.00	97.00	1.47	0.98
CMEN [49]	97.00	96.00	2.14	0.97

UNISA [51]	98.80	98.20	1.98	0.99
IEEE IFS-TC [52]	99.31	98.57	1.00	0.99
Combined (CASIA v1.0, CASIAv2.0 and CoMFoD)	99.21	99.10	0.56	0.99

A. Experimental Results on CASIA v2.0 Dataset

Geometric transformations such as scaling, rotation, and deformation are applied normally in combination or individual on forged regions to hide the cues of forgery. These transformations are applied on copy-move forged region(s) in the CASIA v2.0 dataset. The detail of rotation, scaling can be seen in [44]. Figure 5 shows the accuracy of the method against these transformations.

The changes along the boundary possess different noise patterns when geometric transformations are applied to the forged region(s). The method performs well with respect to different geometric transformations because these changes are modeled properly by estimating and encoding the distribution of noise precisely.

Forgeries using different size regions introduce variations in noise patterns which are usually consistent in unaltered images. The method is explored on small (30 % of image size), medium (50% of image size), and large (more than 50% of image size) copy-move forged region(s). Local inconsistencies occurred due to copy-move forged region(s) are useful in exposing forgery [60-61], which are exposed effectively in our method. Figure 6 shows the results with these sizes.

Copy or cut pasting of different types of shapes/objects in images from the same or different images is very common to gain illegal benefits. CASIA v2.0 datasets contain the four region shapes: circular (CR), rectangular (RECT), triangular (TRI), and arbitrary (ARB), which are pasted to other locations images. The method is robust on different shapes of the pasted region(s). Figure 7 shows the results with these shapes.

B. Experimental Results on CoMFod Dataset

Many post-processing operations such as scaling, rotation, JPEG compression, blurring, color reduction (CR), brightness change (BC), contrast adjustments (CA), and noise adding (NA) are commonly used to hide the traces of tampering [59]. In the CASIA v2.0 dataset, only image blurring (along and within the boundary of tampered regions) is applied after crop and paste operation to hide the cues of tampering.

We performed additional experiments using the CoMFoD dataset to ensure the robustness against post-processing operations because it has 10400 post-processed authentic and forged images with a variety of post-processing operations such as JPEG compression, blurring, noise adding (NA), brightness change (BC), color reduction (CR), and contrast adjustment (CA). The experimental results (see Figure 8) show the robustness of our method against different post-processing operations on the CoMFoD dataset. The results show the significance of the FFT-DRLBP descriptor.

C. Experimental Results on CoMFod Dataset

To validate the robustness of the proposed method against post-processing operations, we created 1056 authentic and 1056 forged images by applying JPEG re-compression, additive noise, blurring, contrast adjustment, and scaling operations on 48 authentic and respective tampered versions of the IMD dataset. The results at different levels of operations are presented in Table IV.

D. Comparison with the state-of-the-art

In this section, a comparison with recent state-of-the-art image forgery methods is presented and analyzed. This comparison is evidence that the proposed method results are better than other methods (see Table V). Our method compares well with recent methods in [15], [62], [65], [68] in terms of ACC, TPR, FPR, and AUC on the CASIA v2.0 dataset. The method in [62] also used DCT-LBP to model the tampering traces. The reason to use DCT and Markov in [15] and [62] together with LBP is to combine edge information together with texture information to produce discriminative features.

We employed the FTT-DRLBP feature extraction strategy to model artifacts of forgery (i.e., noise and edges) in a single representation to get significant features by eliminating the need for feature reduction as compared to [15] and [62]. To compare the results of the proposed method on the CoMFoD dataset (see Table V), we implemented the method in [15], [30], [65] and performed experiments using the CoMFoD dataset.

The comparison (see Table V) shows that the proposed approach has better performance than the method [69] in terms of *TPR*. The reason for significant results is that the FFT-DRLBP feature extraction strategy produced discriminative features. The results of the method are comparable with methods in [29], [46] for forgery detection on the GRIP dataset (see Table V). The method has significant performance improvement over the methods in [29], [46] on the GRIP dataset even in the presence of JPEG compression, noise adding, and rescaling.

Results show that the method has significant performance on different levels of post-processing operations. All methods have a good performance on high JPEG compression. The proposed method has better performance even on low JPEG compression. Similarly, the performance of the proposed method is better on a high level of noise and rescaling. The proposed method performance is also improved than methods [67-68].

The methods in [2-3], [28] have encouraging results on forensic analysis using noise features. These methods are evaluated on images/datasets which are designed specifically to evaluate the image manipulations such as JPEG compression, contrast enhancement, brightness adjustment, etc.

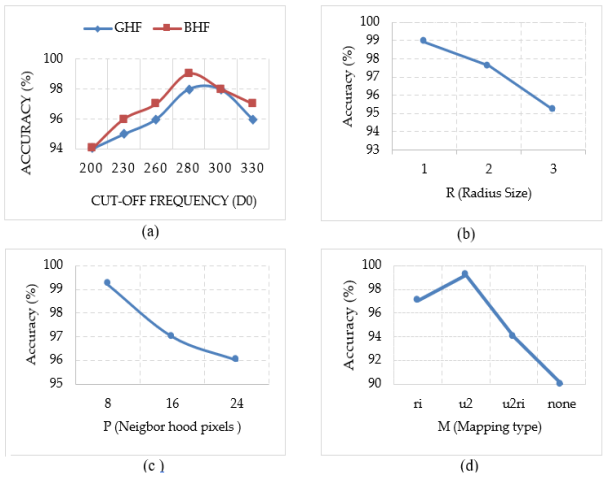


Figure 4. Effect of various parameters on accuracy (%), (a) Effect of D_0 parameter, (b) Effect of different radius, (c) Effect of the various number of neighborhood pixels (P), (d) Effect of various types of mapping (M)

TABLE IV. ROBUSTNESS AGAINST POST- PROCESSING OPERATIONS AT DIFFERENT LEVELS

Post-Processing Operation	Level	ACC (%)	TPR (%)	FPR (%)	AUC
JPEG re-compression	100	99.00	99.21	0.68	0.99
	90	98.00	98.21	1.68	0.98
	80	96.00	97.13	2.43	0.97
	70	96.00	97.12	2.42	0.97
	60	94.00	95.11	4.42	0.95
	50	94.00	95.11	4.42	0.95
Noise ($\mu = 0$)	$\sigma2$=0.009	98.00	97.43	1.52	0.98
	$\sigma2$=0.005	98.00	98.86	1.32	0.98
	$\sigma2$=0.0005	99.71	99.44	0.42	0.99
Blurring	3×3	98.21	97.11	3.42	0.96
	5×5	94.21	95.11	3.42	0.95
	7×7	90.71	91.56	8.32	0.91
Brightness Change	(0.01,0.95)	96.34	97.43	2.32	0.97
	(0.01,0.90)	97.11	98.14	2.13	0.97
	(0.01,0.80)	96.11	97.00	3.00	0.96
Scaling	0.5	40.00	46.00	33.00	0.50
	1	99.00	99.23	0.71	0.99
	1.5	60.00	63.32	31.22	0.61
Contrast Adjustment	(0.01,0.95)	96.11	97.14	3.13	0.97
	(0.01,0.9)	98.00	98.44	2.52	0.98
	(0.01,0.8)	97.00	96.00	4.00	0.96

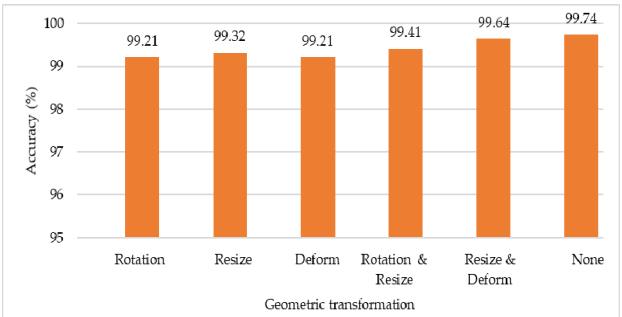


Figure 5. Proposed method accuracy on images with different geometric transformations on CASIA v2.0 dataset

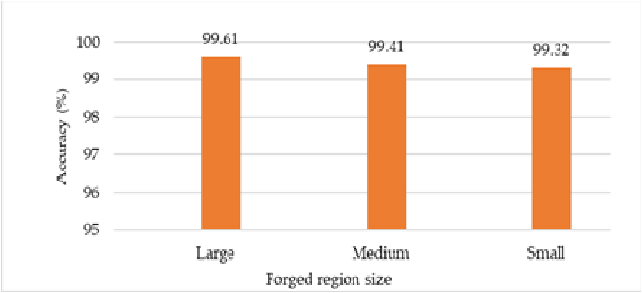


Figure 6. Proposed method accuracy on different sizes of forged regions on CAISA v2.0 dataset

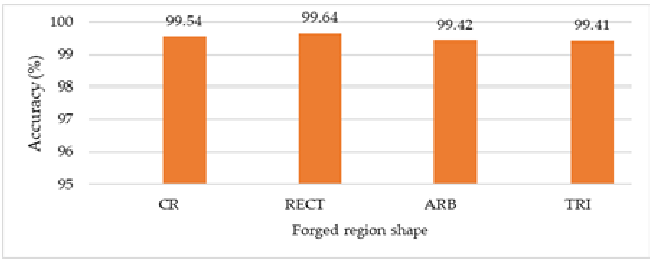


Figure 7. Proposed method accuracy on different shapes of forged regions/objects on CASIA v2.0 dataset

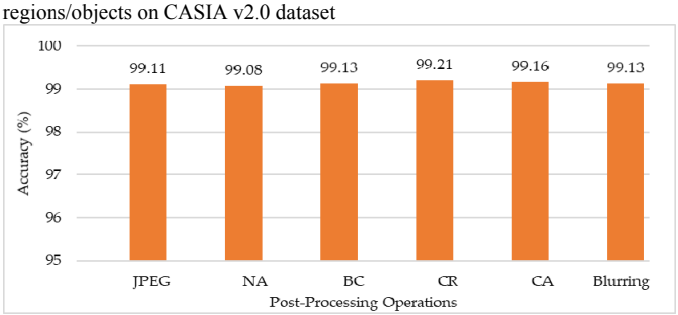


Figure 8. Proposed method accuracy on different post-processing operations on CoMFoD dataset

TABLE V. COMPARISON OF PROPOSED METHOD WITH OTHER STATE-OF-THE-ART METHODS

Datasets	Approaches	ACC (%)	TPR (%)	FPR (%)	AUC
SIA v1.0	Alahmadi et al., [62]	97.00	98.24	--	0.97
	Shen et al., [63]	97.00	--	--	--
	Alfy and Qureshi [15]	98.65	98.80	--	0.99
	Goh and Thing [64]	90.18	--	--	--
	Hussain et al., [65]	96.53	--	--	--
	Muhammad et al., [66]	94.89	93.91	--	0.93
	Rao et al., [67]	98.04	--	--	--
	Pham et al., [68]	96.90	--	--	--
	Proposed	98.96	99.03	--	0.98
CASIA v2.0	Jalab et al., [69]	99.54	95	--	--
	Alfy et al., [15]	99.00	99.55	0.45	0.99
	Alahmadi et al., [62]	97.50	98.45	3.16	0.97
	Hussain et al., [65]	96.52	96.02	4.98	0.97
	Pham et al., [68]	96.90	--	--	--
	Proposed	99.54	99. 82	0.39	0.99
CoMFoD	Wang et al., [30]	99.00	98.92	1.90	0.98
	Hussain et al., [65]	96.52	96.02	4.98	0.97
	Alfy et al., [15]	98.23	97.92	2.00	0.98
	Proposed	99.13	98.13	0.99	0.99
MICC-F220	Al_Azrak et al., [70]	100.00	--	--	--
	Khurshid et al., [41]	99.64	99.9	--	0.99
	Amerini et al., [48]	--	98.21	--	--
	Wang and Kamata [30]	98.92	--	--	--
	Proposed	99.74	99.85	0.78	0.99
GRIP	Yang et al., [29]	89.52	--	--	--
	Cozzolino et al., [46]	94.61	--	--	--
	Proposed	97.00	98.11	2.47	0.98

TABLE VI. COMPARISON WITH STATE-OF-THE-ART AND PROPOSED METHOD ON CROSS DATASET

Training Dataset	Testing Dataset	Proposed		Alfy et al., [15]		Hussain et al., [65]		Wang et al., [30]	
		ACC	FPR	ACC	FPR	ACC	FPR	ACC	FPR
CASIA v1. 0, CASIA v2.0 & CoMFoD	DWIF [47]	80.78	13.67	70.23	20.29	78.87	18.35	78.87	18.35
	MICC-F220 [48]	86.16	12.02	81.34	16.33	76..11	21.05	82.05	19.35
	IMD [49]	87.37	10.58	83.45	13.52	78.31	22.35	82.45	16.55
	CMH [50]	86.77	9.58	82.73	11.76	79.47	19.19	83.67	17.19
	CMEN [49]	85.47	12.00	81.36	17.00	76.32	23.00	80.74	19.95
	UINSA [71]	86.26	8.58	80.43	15.03	75.21	20.19	84.21	10.44
	IEE IFS-TC [52]	86.15	8.18	79.13	17.33	74.12	22.91	83.21	11.94
	WWTI [53]	81.39	12.15	79.13	17.33	73.42	19.91	72.31	20.94

E. Cross Dataset Validation

Cross dataset experiments are performed to validate the proposed approach because in real applications source of the image is not known. For this purpose, three state-of-the-art methods [15], [30], 65] are implemented together with the proposed approach. For cross dataset validation, we used a pre-trained SVM classifier, which is trained on images of combined datasets (CASIA v1.0, CASIA v2.0, and CoMFoD). The cross datasets results are shown in Table VI (ACC etc., are quantified in percentage values).

Usually, the same dataset is divided into two parts for training and testing or k-fold strategy on the same dataset. The method has reasonable performance when it is tested on unknown datasets for which it has no prior knowledge. The better accuracy is achieved through the proposed method due to the discriminated nature of the features obtained through the proposed descriptor.

VI. CONCLUSION

We introduced a passive method for image forgery detection based on the hypothesis that noise patterns are consistent throughout the image if it is not altered; the method achieved promising results. FFT with high pass filtering is used to estimate noise patterns. A robust texture descriptor DRLBP is employed to analyze the estimated noise patterns for detecting inconsistency in noise patterns. The analysis of the FFT-DRLBP descriptor is passed to SVM for final decision making. FFT-DRLBP descriptor enables the method to detect copy-move image forgery even in the presence of post-processing operations. Intensive experiments were performed on benchmark public datasets using 10-fold cross-validation to evaluate the method and ensure its robustness; it achieved an average accuracy of 99.21%. Comparison with the state-of-the-art methods showed that it works well to detect the copy-move forgeries and detects the tampered images gone under different post-processing operations to hide the cues of tampering. It was also evaluated using cross-dataset validation (training and testing on different datasets); it achieved encouraging results. The method significantly outperforms the state-of-the-art methods in cross-dataset scenarios, which is important in real situations where classifiers cannot always be trained on images from the domain, where analysis is to be performed for forgery detection. In future work, the focus will be to improve the cross-dataset validation by finding stronger features using deep learning techniques.

REFERENCES

[1] R. Pandey, S. Singh, and K. Shukla, "Passive forensics in image and video using noise features: A review," Digital Investigation, vol. 19, pp. 1-28, 2016. doi:10.1016/j.diin.2016.08.002

[2] H. Gou, A. Swaminathan, and M. Wu, "Noise features for image tampering detection and steganalysis," in IEEE International Conference on Image Processing, San Antonio, Texas, USA, 2007, pp. 97-100. doi:10.1109/ICIP.2007.4379530

[3] J. Fan, H. Cao, and A. C. Kot, "Estimating EXIF parameters based on noise features for image manipulation detection," IEEE Transactions on Information Forensics and Security, vol. 8, pp. 608-618, 2013. doi:10.1109/TIFS.2013.2249064

[4] Y. Ke, C. Zhang, M. Qiang, Z. Weidong and Shuguang, "Detecting image forgery based on noise estimation," International Journal of Multimedia and Ubiquitous Engineering, vol. 9, pp. 325-336, 2014. doi:10.14257/ijmue.2014.9.1.30

[5] C. M. Pun, B. Liu, and X. C. Yuan, "Multi-scale noise estimation for image splicing forgery detection," Journal of Visual Communication and Image Representation, vol. 38, pp. 195-206, 2016. doi:10.1016/j.jvcir.2016.03.005

[6] J. Lukáš, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," in Security, Steganography, and Watermarking of Multimedia Contents VIII, 2006, p. 60720Y. doi:10.1117/12.640109

[7] C.-C. Hsu, T.-Y. Hung, C.-W. Lin, and C.-T. Hsu, "Video forgery detection using correlation of noise residue," in 2008 IEEE 10th workshop on multimedia signal processing, 2008, pp. 170-174

[8] X. Pan, X. Zhang, and S. Lyu, "Exposing image forgery with blind noise estimation," in Proceedings of the thirteenth ACM multimedia workshop on Multimedia and security, 2011, pp. 15-20

[9] C. Liu, R. Szeliski, S. B. Kang, C. L. Zitnick, W. T. Freeman, "Automatic estimation and removal of noise from a single image," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 30, pp. 299-314, 2007. doi:10.1109/TPAMI.2007.1176

[10] C. Liu, W. T. Freeman, R. Szeliski, and S. B. Kang, "Noise estimation from a single image," in IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'06), 2006, pp. 901-908. doi:10.1109/CVPR.2006.207

[11] B. Goyal, A. Dogra, S. Agrawal, B. Sohi, and A. Sharma, "Image denoising review: From classical to state-of-the-art approaches," Information Fusion, vol. 55, pp. 220-244, 2020. doi:10.1016/j.inffus.2019.09.003.

[12] [12] A. Khurshid, G. Ghulam , S. Mubbashar, and H. Zulfiqar, "Automatic enhancement of digital images using Cubic Bézier Curve and Fourier transformation," Malaysian Journal of Computer Science, vol. 30, pp. 300-310, 2017. doi:10.22452/mjcs.vol30no4.3

[13] A. Satpathy, X. Jiang, and H. L. Eng, "LBP-based edge-texture features for object recognition," IEEE Transactions on Image Processing, vol. 23, pp. 1953-1964, 2014. doi:10.1109/TIP.2014.2310123

[14] A. Khurshid, H. Zulfiqar, and H. Muhammad, "Copy-move and splicing image forgery detection and localization techniques: a review," Australian Journal of Forensic Sciences, vol. 49, pp. 281-307, 2017. doi:10.1080/00450618.2016.1153711

[15] E.-S. M. El-Alfy and M. A. Qureshi, "Robust content authentication of gray and color images using lbp-dct markov-based features," Multimedia Tools and Applications, vol. 76, pp. 1-22, 2016. doi:10.1007/s11042-016-3855-7

[16] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in 18th International Conference on Pattern Recognition,(ICPR), Hong Kong, 2006, pp. 746-749. doi:10.1109/ICPR.2006.1003

[17] S. Bayram, H. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Taipei, Taiwan, 2009, pp. 1053-1056. doi:10.1109/ICASSP.2009.4959768

[18] B. Mahdian and S. Saic, "Blind methods for detecting image fakery," IEEE Aerospace and Electronic Systems Magazine, vol. 25, pp. 18-24, 2010. doi:10.1109/CCST.2008.4751315

[19] Y. Wu, Y. Deng, H. Duan, and L. Zhou, "Dual tree complex wavelet transform approach to copy-rotate-move forgery detection," Science China Information Sciences, vol. 57, pp. 1-12, 2014. doi:10.1007/s11432-013-4823-8

[20] F. Peng, Y.-y. Nie, and M. Long, "A complete passive blind image copy-move forensics scheme based on compound statistics features," vol. 212, pp. e21-e25, 2011. doi:10.1016/j.forsciint.2011.06.011

[21] R. C. Pandey, S. K. Singh, and K. K. Shukla, "A passive forensic method for video: Exposing dynamic object removal and frame duplication in the digital video using sensor noise features," Journal of Intelligent Fuzzy Systems, vol. 32, pp. 3339-3353, 2017. doi:10.3233/JIFS-169275

[22] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in Information Hiding, 2004, pp. 395-407.doi:10.1007/978-3-540-30114-1_10

[23] H. Gou, A. Swaminathan, and M. Wu, "Noise features for image tampering detection and steganalysis," in 2007 IEEE International Conference on Image Processing, 2007, pp. VI-97-VI-100

[24] B. Mahdian and S. Saic, "Using noise inconsistencies for blind image forensics," Image and Vision Computing, vol. 27, pp. 1497-1503, 2009. doi:10.1016/j.imavis.2009.02.001

[25] X. Kang, Y. Li, Z. Qu, and J. Huang, "Enhancing source camera identification performance with a camera reference phase sensor pattern noise," IEEE Transactions on Information Forensics and Security, vol. 7, pp. 393-402, 2012. doi:10.1109/TIFS.2011.2168214

[26] M. C. Stamm and K. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," IEEE Transactions on Information Forensics and Security, vol. 5, pp. 492-506, 2010. doi:10.1109/TIFS.2010.2053202

[27] B. Liu, C. M. Pun, and X. C. Yuan, "Digital image forgery detection using JPEG features and local noise discrepancies," The Scientific World Journal, vol. 14, pp. 1-12, 2014. doi:10.1155/2014/230425

[28] G. Chierchia, G. Poggi, C. Sansone, and L. Verdoliva, "A Bayesian-MRF approach for PRNU-based image forgery detection," IEEE Transactions on Information Forensics and Security, vol. 9, pp. 554-567, 2014. doi:10.1109/TIFS.2014.2302078

[29] H. Y. Yang, Y. Niu, L. Jiao, Y. Liu, X. Wang, and Z. Zhou, "Robust copy-move forgery detection based on multi-granularity Superpixels matching," Multimedia Tools and Applications, pp. 1-27, 2017. doi:10.1007/s11042-017-4978-1

[30] L. Wang and S.-i. Kamata, "Forgery image detection via mask filter banks based CNN," in 10th International Conference on Graphics and Image Processing, Chengdu, China, 2019, pp. 1-6. doi:10.1117/12.2524351

[31] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in IEEE conference on computer vision and pattern recognition, Las Vegas, Nevada, USA, 2016, pp. 770-778. doi:10.1109/CVPR.2016.90

[32] V. Mall, K. Bhatt, S. K. Mitra, and A. K. Roy, "Exposing structural tampering in digital images," in 2012 IEEE International Conference on Signal Processing, Computing and Control, 2012, pp. 1-6. doi:10.1109/ISPCC.2012.6224369

[33] G. Gilanie, U. I. Bajwa, M. M. Waraich, Z. Habib, H. Ullah, and M. Nasir, "Classification of normal and abnormal brain MRI slices using Gabor texture and support vector machines," Signal, Image and Video Processing, vol. 12, pp. 479-487, 2018. doi:10.1007/s11760-017-1182-8

[34] G. Gilanie, N. Nasir, U. I. Bajwa, and H. Ullah, "RiceNet: convolutional neural networks-based model to classify Pakistani grown rice seed types," Multimedia Systems, pp. 1-9, 2021. doi:10.1007/s00530-021-00760-2

[35] M. Saddique, K. Asghar, U. I. Bajwa, M. Hussain, H. A. Aboalsamh, and Z. Habib, "Classification of authentic and tampered video using motion residual and parasitic layers," IEEE Access, vol. 8, pp. 56782-56797, 2020. doi:10.1109/ACCESS.2020.2980951

[36] R.-E. Precup, T.-A. Teban, A. Albu, A.-B. Borlea, I. A. Zamfirache, and E. M. Petriu, "Evolving fuzzy models for prosthetic hand myoelectric-based control," IEEE Transactions on Instrumentation and Measurement, vol. 69, pp. 4625-4636, 2020. doi:10.1109/TIM.2020.2983531

[37] I.-D. Borlea, R.-E. Precup, A.-B. Borlea, and D. Iercan, "A unified form of fuzzy C-means and K-means algorithms and its partitional implementation," Knowledge-Based Systems, vol. 214, p. 106731, 2021. doi:10.1016/j.knosys.2020.106731

[38] H. Gou, A. Swaminathan, and M. Wu, "Intrinsic sensor noise features for forensic analysis on scanners and scanned images," IEEE Transactions on Information Forensics Security, vol. 4, pp. 476-491, 2009. doi:10.1109/TIFS.2009.2026458

[39] X. Sun, Y. Li, S. Niu, and Y. Huang, "The detecting system of image forgeries with noise features and EXIF information," Journal of Systems Science and Complexity, vol. 28, pp. 1164-1176, 2015. doi:10.1007/s11424-015-4023-2

[40] C. C. Hsu, T. Y. Hung, C. W. Lin, and C. T. Hsu, "Video forgery detection using correlation of noise residue," in IEEE 10th Workshop on Multimedia Signal Processing, 2008, pp. 170-174. doi:10.1109/MMSP.2008.4665069

[41] K. Asghar, X. Sun, P. L. Rosin, M. Saddique, M. Hussain, and Z. Habib, "Edge–texture feature-based image forgery detection with

cross-dataset evaluation," Machine Vision and Applications, vol. 30, pp. 1243-1262, 2019. doi:10.1007/s00138-019-01048-2

[42] M. Saddique, K. Asghar, U. I. Bajwa, M. Hussain, and Z. Habib, "Spatial video forgery detection and localization using texture analysis of consecutive frames," Advances in Electrical and Computer Engineering, vol. 19, pp. 97-108, 2019. doi:10.4316/AECE.2019.03012

[43] N. Kanwal, A. Girdhar, L. Kaur, and J. S. Bhullar, "Detection of digital image forgery using fast fourier transform and local features," in 2019 International Conference on Automation, Computational and Technology Management (ICACTM), 2019, pp. 262-267. doi:10.1109/ICACTM.2019.8776709

[44] J. Dong and W. Wang, "CASIA image tampering detection evaluation databases," in Signal and Information Processing (ChinaSIP), Beijing, China, 2011, pp. 422-426.doi:10.1109/ChinaSIP.2013.6625374

[45] Christlein, V. Riess, C. Jordan, and J. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," IEEE Transactions on Information Forensics and Security, vol. 7, pp. 1841-1854, 2012. doi:10.1109/TIFS.2012.2218597

[46] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copy–move forgery detection," IEEE Transactions on Information Forensics and Security, vol. 10, pp. 2284-2297, 2015. doi:10.1109/TIFS.2015.2455334

[47] M. Zampoglou and R. Bouwmeester, The Deutsche Welle Image Forensics Dataset [Online]. Available: https://revealproject.eu/the-deutsche-welle-image-forensics-dataset/

[48] 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 Transactions on Information Forensics and Security, vol. 6, pp. 1099-1110, 2011. doi:10.1109/TIFS.2011.2129512

[49] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," IEEE Transactions on Information Forensics and Security, vol. 7, pp. 1841-1854, 2012. doi:10.1007/s11045-019-00688-x

[50] E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes," Journal of Visual Communication and Image Representation, vol. 29, pp. 16-32, 2015. doi:10.1016/j.jvcir.2015.01.016

[51] [51] G. Cattaneo, G. Roscigno, and U. F. Petrillo, "Improving the experimental analysis of tampered image detection algorithms for biometric systems," Pattern Recognition Letters, vol. 113, pp. 93-101, 2017. doi:10.1016/j.patrec.2017.01.006

[52] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, "Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques," in IEEE International Conference on Image Processing (ICIP), 2014, pp. 5302-5306. doi:10.1109/ICIP.2014.7026073

[53] M. Zampoglou, S. Papadopoulos, and Y. Kompatsiaris, "Detecting image splicing in the wild (web)," in IEEE International Conference on Multimedia & Expo Workshops (ICMEW), 2015, pp. 1-6. doi:10.1109/ICMEW.2015.7169839

[54] M. Sokolova, N. Japkowicz, and S. Szpakowicz, "Beyond accuracy, F-score and ROC: a family of discriminant measures for performance evaluation," in Australasian joint conference on artificial intelligence, Berlin, Germany 2006, pp. 1015-1021. doi:10.1007/11941439_114

[55] R. A. Melter, "Some characterizations of city block distance," vol. 6, pp. 235-240, 1987. doi:10.1016/0167-8655(87)90082-1

[56] L. Bai, A. Velichko, and B. W. Drinkwater, "Ultrasonic characterization of crack-like defects using scattering matrix similarity metrics," IEEE transactions on ultrasonics, ferroelectrics, and frequency control, vol. 62, pp. 545-559, 2015. doi:10.1109/TUFFC.2014.006848

[57] J. Y. Hesterman, L. Caucci, M. A. Kupinski, H. H. Barrett, and L. R. Furenlid, "Maximum-likelihood estimation with a contracting-grid search algorithm," IEEE transactions on nuclear science, vol. 57, pp. 1077-1084, 2010. doi:10.1109/TNS.2010.2045898

[58] J. Byun, H. A. Patel, and C. T. Yavuz, "Magnetic $BaFe_{12}O_{19}$ nanofiber filter for effective separation of Fe_3O_4 nanoparticles and removal of arsenic," Journal of nanoparticle research, vol. 16, p. 2787, 2014. doi:10.1007/s11051-014-2787-2

[59] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD-New database for copy-move forgery detection," in 55th ELMAR International Symposium, Zadar, Croatia, 2013, pp. 49-54. doi:10.1109/ICIP.2016.7532339

[60] B. Mahdian, S. J. I. Saic, "Using noise inconsistencies for blind image forensics," Image and Vision Computing, vol. 27, pp. 1497-1503, 2009. doi:10.1016/j.imavis.2009.02.001

[61] X. Pan, X. Zhang, and S. Lyu, "Exposing image splicing with inconsistent local noise variances," in IEEE International Conference on Computational Photography (ICCP), 2012, pp. 1-10. doi:10.1109/ICCPhot.2012.6215223

[62] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and H. Mathkour, "Passive detection of image forgery using DCT and local binary pattern," Signal, Image and Video Processing, vol. 11, pp. 81-88, 2017. doi:10.1007/s11760-016-0899-0

[63] X. Shen, Z. Shi, and H. Chen, "Splicing image forgery detection using textural features based on the grey level co-occurrence matrices," IET Image Processing, vol. 11, pp. 44-53, 2016. doi:10.1049/iet-ipr.2016.0238

[64] J. Goh and V. L. Thing, "A hybrid evolutionary algorithm for feature and ensemble selection in image tampering detection," International Journal of Electronic Security and Digital Forensics, vol. 7, pp. 76-104, 2015. doi:10.1504/IJESDF.2015.067996

[65] M. Hussain, S. Qasem, G. Bebis, G. Muhammad, H. Aboalsamh, and H. Mathkour, "Evaluation of image forgery detection using multi-scale weber local descriptors," International Journal on Artificial Intelligence Tools, vol. 24, pp. 1-28, 2015. doi:10.1142/s0218213015400163

[66] G. Muhammad, M. Al-Hammadi, M. Hussain, and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," Machine Vision and Applications, vol. 25, pp. 985-995, 2014. doi:10.1109/KBEI.2015.7436195

[67] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in IEEE International Workshop on Information Forensics and Security (WIFS), 2016, pp. 1-6. doi:10.1109/WIFS.2016.7823911

[68] N. T. Pham, J.-W. Lee, G.-R. Kwon, and C.-S. Park, "Efficient image splicing detection algorithm based on markov features," Multimedia Tools and Applications, pp. 1-15, 2018. doi:10.1007/s11042-018-6792-9

[69] H. A. Jalab, T. Subramaniam, R. W. Ibrahim, H. Kahtan, and N. F. M. Noor, "New Texture Descriptor Based on Modified Fractional Entropy for Digital Image Splicing Forgery Detection," Entropy, vol. 21, p. 371, 2019. doi:10.3390/e21040371

[70] F. M. Al_Azrak, A. Sedik, M. I. Dessowky, G. M. El Banby, A. A. Khalaf, A. S. Elkorany, and F. E. A. El-Samie, "An efficient method for image forgery detection based on trigonometric transforms and deep learning," Multimedia Tools and Applications, pp. 1-23, 2020. doi:10.1007/s11042-019-08162-3

[71] G. Cattaneo, G. Roscigno, and U. F. Petrillo, "Improving the experimental analysis of tampered image detection algorithms for biometric systems," Pattern Recognition Letters, vol. 113, pp. 93-101, 2018. doi:10.1016/j.patrec.2017.01.006