Pamukkale Univ Muh Bilim Derg, 28(5), 748-760, 2022

Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi

Pamukkale University Journal of Engineering Sciences

Copy-Move forgery detection and localization with hybrid neural network approach

Hibrit sinir ağı yaklaşımı ile kopyala-taşı sahteciliği tespiti ve lokalizasyonu

Gül TAHAOĞLU[1*], *Guzin ULUTAS*[1]

[1]Department of Computer Engineering, Engineering Faculty, Karadeniz Technical University, Trabzon, Turkey.
tahaoglugul@gmail.com, gulutas@ktu.edu.tr

Received/Geliş Tarihi: 31.05.2021 Revision/Düzeltme Tarihi: 20.12.2021 doi: 10.5505/pajes.2022.88714
Accepted/Kabul Tarihi: 31.01.2022 Research Article/Araştırma Makalesi

Abstract

Copy-move forgery, in which copied a region of the image and pasted onto another region on the same image, is the most encountered image forgery technique recently. Many frameworks have been presented to detect such forgeries. The main drawback with these approaches is their performance can be degraded when the duplicated image has undergone ~~to~~ some attacks. In this work, it is aimed to propose a hybrid approach, which uses deep features and DCT-based block features in a combined manner, to achieve higher detection performance even ~~if~~ under various attack scenarios. The proposed method uses a global contrast correction technique called LDR during the preprocessing phase and then extracts deep features from the image patches using a deep neural network. The method also obtains block features from the image to robustness against JPEG compression attacks. Hybrid features (deep and block-based features) are matched using Patch Match and then the proposed post-processing operation is realized on the matching results to minimize false matches. According to empirical studies performed on available databases, the proposed scheme gives better results when compared to both keypoint-based and block-based references even under attacks with challenging parameters.

Keywords: Copy-move forgery, Deep based features, Hybrid features, Patch based matching.

Öz

Görüntünün bir kısmının kopyalayıp aynı görüntü üzerinde başka bir bölgeye bölge gizlemek veya çoğaltmak amacıyla yapıştırılarak oluşturulan kopya-taşı sahteciliği, son yıllarda en çok karşılaşılan görüntü sahteciliği tekniğidir. Literatürde bu tür sahtecilikleri tespit etmek için birçok çalışma önerilmiştir. Bu yaklaşımların ana dezavantajı, sahte görüntü bazı işleme öncesi veya sonrası saldırılara maruz kaldığında performanslarının düşebilmesidir. Bu çalışmada, derin öznitelikler ile DCT tabanlı blok özniteliklerinin bir arada kullanıldığı hibrit bir yaklaşım ile çeşitli saldırı senaryolarında dahi daha iyi tespit oranlarının elde edilmesi amaçlanmaktadır. Önerilen yöntem, ön işleme aşamasında LDR adı verilen global bir kontrast düzeltme tekniği kullanır ve daha sonra derin bir sinir ağı kullanarak görüntü yamalarından derin öznitelikler çıkarır. Yöntem ayrıca, yöntemi JPEG sıkıştırma saldırılarına karşı daha sağlam hale getirmek için görüntüden blok özellikleri alır. Hibrit özellikler (derin ve blok tabanlı özellikler) Yama Eşleştirme kullanılarak eşleştirilir ve ardından yanlış eşleşmeleri en aza indirmek için eşleştirme sonuçları üzerinde önerilen son işleme işlemi gerçekleştirilir. Mevcut veri tabanları üzerinde gerçekleştirilen deneysel çalışmalara göre önerilen şema, yüksek oranda parametrelerle yapılan saldırılar altında bile hem anahtar nokta tabanlı hem de blok tabanlı referanslara kıyasla daha iyi sonuçlar vermektedir.

Anahtar kelimeler: Kopyala-taşı sahteciliği, Derin öznitelikler, Hibrit öznitelikler, Yama tabanlı eşleşeme.

1 Introduction

Malicious users can make image forgery easily by using free image editing tools, even if they have not any skill on this topic. For this reason, authentication of the images becomes important. The methods are split into two categories: Active methods and passive methods. The approaches in the first category need special information called a watermark or signature to authenticate the image. Other types of methods that utilize only statistical information of the image, do not require extra information. Furthermore, images that are captured by specially equipped hardware can be authenticated by the active methods. Passive methods have become popular among researchers because they do not need any extra information for authentication. In addition to passive image forgery detection methods, there are also passive video forgery methods in the literature [48]. Passive image forgery detection methods can be classified into two subclasses, image splicing detection techniques, and copy-move forgery detection (CMFD) techniques. The former one is used for the detection of a special forgery type, which copies a portion on an image and pastes it onto a region on another image. Techniques in the latter class deal with copy-move forgery operation which copy part of an image and paste it on the same image. This forgery operation aims to cover or replicate some objects or regions on the image. This type of forgery mostly goes unnoticed by users. Figure 1 shows a sample of copy-move forgery images. In Figure 1(a), the authentic image is given and in (b) forged version of the image is given.

A lot of methods have been proposed recently for CMFD and studies on this problem continue to increase. We can classify all the works in this area into two categories as suggested by [1]; Block-based and keypoint-based schemes. Block-based ones split the input image into square/circular overlapping/nonoverlapping subblocks. The researchers have used various feature extraction methods to obtain distinctive features vectors of image subblocks. The obtained vectors are sorted lexicographically to make comparable vectors closer to each other.

*Corresponding author/Yazışılan Yazar



(a): Unforged one.



(b): Forged one.

Figure 1. A sample of copy move forgery.

Duplicated regions are revealed by the methods after the matching process, which decides the similarity of the vector using Euclidean distance. Some of the existing methods include filtering steps to minimize possible false matches and to obtain better performance. The feature extraction and matching stages in these methods lead to high run time, so researchers introduce the keypoint-based methods to overcome this problem. This type of forgery detection scheme becomes robust geometric distortion attacks. The basic steps of these methods are obtaining keypoints and matching ~~of~~ them. The main disadvantage of these studies is they do not have enough performance if the forged regions have smooth characteristics.

In this study, it is presented a novel CMFD method after analyzing popular CMFD methods including both traditional and deep learning-based methods. A key contribution of this study is to obtain the learned features from the mid-level of trained CNN architecture and to obtain the frequency features of the image blocks to make the method more resistant to attacks with high parameters, so handcrafted features and deep features are used in a hybrid manner. Furthermore, as preprocessing step, to perform forgery detection with higher accuracy even in low contrast images, Layered Difference Representation (LDR), which is used to the layered difference representation of 2D histograms, is used to improve the contrast of the input image. One of the popular copy-move forgery database named GRIP is utilized in experiments. The experiments reveal that the proposed scheme has better detection performance under both image degradation attacks and geometric distortion attacks.

1.1 Related works

In this section, works in the CMFD area are analyzed in the three subsections. Block-based, keypoint-based, and deep learning-based methods are given with details in Figure 1.

1.1.1 Block-based methods

Methods in the first category split the input image overlapping or nonoverlapping subblocks. Features of each block are extracted to represent them and then lexicographically sorted to provoke the similar vectors closer. The matching phase of the methods determines possible forgeries by using similarity distance between feature vectors. Many methods in literature by using various approaches are proposed to obtain block features. The first method in CMFD used the Discrete Cosine Transform (DCT) on 8x8 overlapping squared blocks to extract features [2]. After the lexicographically sorting process on the feature vectors, Euclidean distance is calculated between neighboring vectors to match them. Following this study, it is proposed to use Principal Component Analysis to decrease the size of feature vector used in [3]. Their method can also reveal forgeries that are exposed to noise addition, JPEG compression, and blurring attacks. After this method, many block-based methods have been proposed until 2015 [4]-[11]. The main difference between them has used feature extraction techniques from overlapping blocks. In [12], it is proposed to use the Patch Match approach in the matching scheme. They analyzed the proposed matching scheme with different feature extraction methods such as FMT, PCT, Zernike moments with polar and cartesian sampling. They reported that the best results were obtained by using Zernike moments with polar sampling. After this method, block-based forgery detection methods continued to be proposed. Bi and others proposed to use Multilevel Dense Descriptor to determine block features [13]. In the first level of the feature extraction step, color texture descriptors are extracted, and then invariant moments are obtained to represent features. Similar descriptors are determined by hierarchical feature matching [14]. Bi and others [15] enhanced the Patch Match algorithm in two viewpoints. And they also suggested the priority-based matching stage based on the reflective offset and the position priority. Bi et. al. also proposed using a coherency-sensitive hashing method to obtain feature vectors of images [16]. To refine feature correspondences, it is proposed to calculate local bidirectional coherency error with an iterative search. If the difference of the local bidirectional coherency error is smaller than the predefined threshold, the iterative search stops. That means the feature correspondences are stable. The stable feature correspondences provide to reveal copy-move forgery regions. Meena and Tyagi used Tartolet transform to extract block feature [51]. The feature vectors sorted lexicographically are matched with the Euclidean distance-based matching approach. In the experiments of the method, some images were selected from the GRIP dataset and the Comofod dataset. In the experiments, the performance result in attack situations is given over only one image. Experimental studies have been kept quite inadequate. Wang et. al. also proposed to use Polar Complex Exponential Transform (PCET) to obtain feature vectors from image subblock [52]. They used Singular Value Decomposition (SVD) to reduce feature dimension and it is also used Particle Swarm Optimization (PSO) and block histogram to find the optimum similarity threshold. The matching of the

blocks was achieved with the optimum threshold found. In the experiments, forged images in Comofod and CASIA datasets were used, and no pixel-level evaluation was made, only image-level forgery detection was performed.

If general speaking, block-based methods have high running time and they do not robust to geometric attacks with high parameters. To overcome of these problems, CMFD with keypoints is proposed. The next part will give a comprehensive analysis of the works in this area.

1.1.2 Keypoint-based methods

Huang and others presented the first keypoint-based CMFD techniques that use the Scale Invariant Feature Transform (SIFT) keypoints [17]. It is suggested to use the best bin first nearest neighbor approach to finding out similar keypoints. In another study, it is proposed to use the SIFT keypoint extraction algorithm with a more comprehensive work than the previous keypoint-based study [18]. They extracted the transformation matrix via matched keypoints by using RANSAC after matching keypoints to localize the forged regions. In [19], it is proposed to use the J-Linkage approach afterward matching steps [19]. In [20], it is proposed to use SURF (Speeded-Up Robust Features) technique in keypoint extraction step [20]. The authors used the nearest neighbor search to match keypoints via their descriptors. The method has not good performance on the detection of forgeries with small regions. In [21], the authors analyzed different features both keypoint-based and block-based features. The features are matched with the k-d tree approach. According to experimental results, SIFT-based methods can be very effective with low computational cost and good performance. In 2015, the authors utilized from Oriented Fast and Robust Brief approach to obtain keypoints [22]. They used Hamming distance for feature vector comparison because Brief is a binary descriptor that is the result of ORB. Li and others presented a new framework, which is used a segmentation approach [23]. They firstly segmented the suspected image into patches after that keypoints are extracted by SIFT. The method realizes a matching operation on the keypoints, which are located on different segments. Another segmentation based CMFD method is presented by Pun and others [24]. Their framework also integrates a block-based approach with a keypoint-based approach. The method firstly segments the image. Keypoints extracted from blocks are evaluated as block features and then matched. The main aim of the first stage in this category can be summarized to obtain higher performance in the next steps.

Shi and others utilized Particle Swarm Optimization (PSO) algorithm to optimize parameters used by SIFT [25]. Generally, the authors determine the parameters experimentally. However, chosen parameters determined by using few images cannot be the right choice for other images. Zandi and others proposed an iterative improvement strategy to obtain keypoints especially for CMFD problems [26]. In another method, KAZE and SIFT keypoints are combined with the hybrid manner in 2017 [27]. The proposed scheme also used the n-best matched algorithm after fusion of keypoints and the possible false matches are eliminated with the RANSAC algorithm. Another method aimed to overcome the problem of this type of forgery detection methods with a smooth region [28]. It proposed to decrease the contrast threshold in SIFT to increase the number of key points. It has caused an increase in the number of false matches because it reduced the distinctiveness of descriptors. The authors only reported the performance under rotation and scaling attacks on an image level. Another keypoint based forgery detection method is proposed by Yang et. al. based on adaptive keypoints extraction and matching [49]. According to the proposed scheme, the keypoints are extracted via the adaptive uniform distribution threshold. Then Binary Robust Invariant Scalable (BRISK) is used to obtain keypoints' descriptors. False matches are eliminated by using RANSAC and the fast mean-residual normalized intensity correlation (NNPROD) is utilized to locate the tampering regions. In [50], to obtain more keypoint the contrast threshold is decreased, and the input image is scaled. The obtained keypoints are matched via a hierarchical matching scheme. Falsely matched keypoints are eliminated and tampering localization is realized via an iterative localization scheme. In [53], the authors extracted SIFT keypoints from the images represented in L*a*b* and RGB color space. They proposed a new enhanced tampering localization step with dynamic thresholding for matching DCT features.

1.1.3 Deep learning-based methods

The existing CMFD methods aim to improve robustness and to minimize running time by using handcrafted features obtained from the suspected images. Keypoint-based features or block features can be encountered in many areas of computer vision. One of the promising topics of computer vision is deep Convolutional Neural Networks (deep-CNNs) which have been successfully applied to image classification, object detection, image hashing retrieval, etc. by taking advantage of automated learning and features extraction.

CNN features are considered an appropriate choice for the CMFD by using automatically learned features. Some recent CMFD studies, which are published as conference papers, have focused on obtaining features by some deep learning methods [29,30,31]. The first of them proposed a splicing and CMFD method via a deep learning approach [29]. Authors train a supervised CNN, to obtain features for the detection of forgery operations (splicing and copy-move). The labeled patches ($p \times p$) from training images by using a patch-sized sliding window and so 400-D features (5x5x16) are obtained. And then SVM classifier is used for binary classification of the image so only image-level evaluation is considered in this work. Results evaluated image-splicing datasets such as CASIA v1.0, v2.0 and Columbia gray DVMM and comparison made with image splicing methods in the literature.

In [30], the proposed technique adapted the trained model AlexNet, slightly the net structure using small training samples. For this purpose, the authors firstly built a copy-move forgery database. Because the number of forgery images is very small for most existing forgery image databases for this technique. For this purpose, moving the rectangle block from the upper left corner to the center randomly generates the forgery images. After that, the used CNN network is initialized with Caffe architecture trained by ImageNet. At last, the proposed model identifies the suspected image if the upper fine-tuning step is realized. It is the first method that integrated CNN especially for solving the CMFD problem, but it is not robust to the copy-move forgery image of real scenarios.

In another work [31], CNN-based CMFD method is presented. The features of image subblocks are extracted via convolution and max-pooling layers of the trained VGG16 model. For a suspected image of size 256x256x3, the VGG16 convolutional feature extractor generates a feature matrix of size 16x16x512. After that, self-correlation is done to figure out the similarity

between any two feature pixels. The authors proposed a pointwise feature extractor namely 1×1, 3×3 and 5×5 rather than traditional methods that use the handcrafted parameters to reveal matched pairs. Finally, all features are combined to predict forgery masks via the reconstruction of a deconvolutional network. Experimental results on CAISA TIDE v2.0 which has not ground truth of forged images and Syn10K datasets are given by comparing [11],[12],[21] and it is reported that the method has higher performance even under various known attacks like affine transformation, JPEG compression, blurring, etc. As criticism of this study, it can be said that the data sets used in the evaluation are not up-to-date and have not been evaluated in recent studies and the performance evaluation against each type of attack has not been given separately. In [54], the authors proposed a forgery detection system with two approaches. The first approach uses a custom design and the second one uses transfer learning which is based on CNNs.

In custom design, it is proposed five architectures with different depths, convolutional layers with two fully connected layers. In the second design, the features are learned by the VGG-16 pre-trained model, and it is selected the block4_pool layer to display one of its feature maps. In the experimental analysis, the robustness of the method against attacks was not evaluated separately.

1.1.4 Motivations and contributions

The advancement of a deep neural network has been reported to improve image recognition performance compared to traditional feature extraction methods where deep CNNs directly learn the end-to-end mapping of the images. However, studies applying deep CNNs to detect copy-move forgeries show limited performance under various attacks and they did not test on datasets that are popular in this field such as [32] in which the forged more realistic and highly undergone some attacks. Previous methods from these studies have been carried out to detect copy-move forgeries used traditional features, but they performed poorly to detect forgeries under various image degradation and geometric attacks. And some of them are inadequate to detect forgeries with smooth regions. Taken over the whole, efficient features, obtained by neural networks and traditional feature extraction methods can be used in a hybrid way to get better accuracy. In addition to that the proposed preprocessing step and using an efficient matching algorithm, the forgeries can be detected with higher performance. Three primary goals of our study can be listed as follows:

1. Preprocessing: The quality of the input image greatly affects detection performance when the forged image has been exposed to some image processing attacks or attacked region has a smooth characteristic. In this work, a global contrast correction technique called LDR was adapted to regulate the contrast of the input.
2. Hybrid Feature Extraction: The proposed method takes advantage of deep CNN-based and DCT-based features of the input image to reveal duplicated regions more accurately. Deep CNNs are trained on large datasets, which is proven to achieve convincing results to recognize objects in natural images. A pre-trained network on the ImageNet dataset named VGG16 is used to provide us efficient feature vectors [44]. But it is not enough for the proposed approach when some attacks with high parameters are considered (like JPEG compression with quality factor 60). For this purpose, DCT based feature vectors are used to robustness against compression attacks.
3. Feature Matching*:* In this work, the dense features obtained from image subblocks, ensure a higher performance when compared to their keypoint-based methods according to results reported in the literature. Although they have higher processing time, they show poor performance under geometric attacks. To overcome these problems, it is used a modified Patch Match based algorithm reveals dense approximate nearest neighbor matches between image subblocks [12].

The empirical results show that our method outperforms the referenced works on the popular copy-move forgery dataset the GRIP. The rest of the paper is given as follows. In Section 3, the presented method is given in detail with subsections. Then, the method is tested and compared on the online available dataset in Section 4. Lastly, the study is completed with the conclusion section.

2 Proposed method

Here, the details of the proposed method are given, which detects and localizes duplicated regions with a new hybrid approach. The method can be divided into four sub-processes. The preprocessing step of the work enhances the contrast ratio of the method using a global contrast enhancement technique called LDR. Feature extraction techniques are then applied to the contrast-enhanced image. The proposed framework utilizes deep-based features and block-based features to obtain better detection results. Features from two different approaches are then matched inside using the Patch Match algorithm. False match elimination is realized as the last step. In Figure 2, the general step of the method is given. The remainder of this section will give details of the sub-processes.

2.1 Preprocessing step

One of the aims of this work is to detect forgeries with higher performance even the duplicated regions have low contrast. For this purpose, it is proposed to use a global contrast enhancement technique as a preprocessing step to enhance the detection performance of the method.

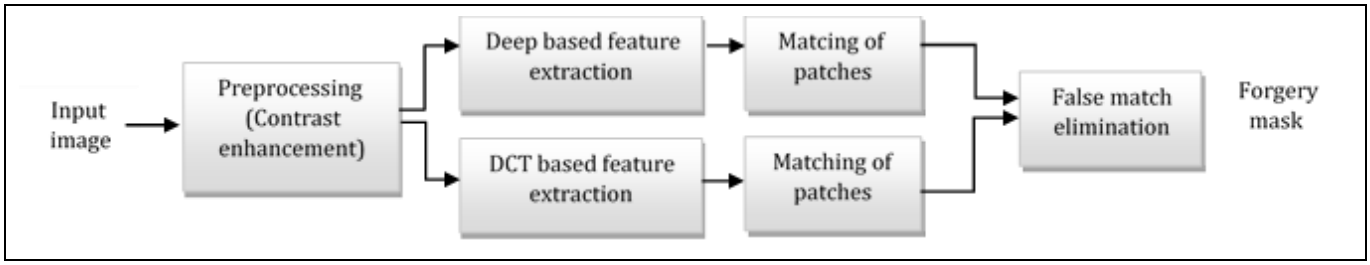


Figure 2. The blog diagram of the proposed novel method.

LDR is used to regulate the contrast of the test image. In this way, input images are improved with having more details and the distinctiveness of the feature vectors to be obtained in the following steps will be increased. Thus, forgeries can be detected easily even with done with smooth regions.

The algorithm aims to enhance image contrast by increasing the difference between the neighboring pixels [34]. For an input image, the algorithm generates a 2D histogram $h(k, k+l)$ by counting pairs of neighboring pixels with gray levels as k and $k+l$. The gray level differences are represented in a layered structure like a tree.

Then, the problem of emphasizing gray level differences in the output image is solved as an optimization problem to derive the transformation function. In Figure 3 the general steps of the algorithm are given.

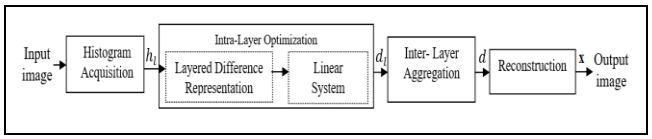
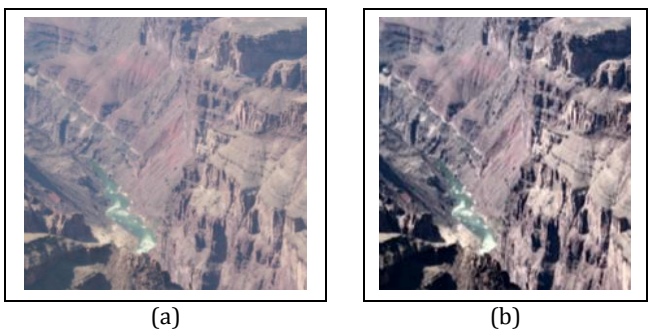


Figure 3. The steps of the used contrast enhancement algorithm [34].

Firstly, the histogram vector at each layer (l) denoted by, is acquired to construct a system of linear equations. The Intra-Layer Optimization step contains two stages named Layered Difference Representation and Linear System. In the first stage, a tree-like pyramidal structure is constituted for each layer, to get an optimum transformation function. For an 8-bit imaging system, the transformation function is represented as x=With this function, assuming *k* and *k+l* are adjacent pixels in the input image, they are mapped to and in the output image. And the next stage is realized to formulate a system of linear equations. At the end of this stage, we acquire the difference vector for each layer. In the Inter-Layer Aggregation step, obtained difference vectors are combined into unique difference vector *d*. Finally, a transformation function is reconstructed by d and the input image is transformed to output image using transformation function x.

In our method, the contrast enhancement algorithm gets the forged image as an input image. By using this method, it is aimed to overcome the common problems of lower performance for detecting copy-move forgery done with low contrast regions. While a doctored image is presented in Figure 4(a), its contrast-enhanced version of it is presented in (b).



(a) (b)

Figure 4(a): Forged image. (b): Obtained image using the contrast enhancement approach.

2.2 Feature extraction step

In this step of the algorithm, two different approaches are used during feature extraction. Deep CNN-based features and DCT based block features are used in a hybrid manner to make the method more robust against various conditions. It is aimed to take advantage of the promising results of deep CNNs for the detection of natural images and to make the system more robust against image degradation attacks by using DCT based features.

2.2.1 Deep based feature extraction

Recently, because of having excellent performance in many computer visions tasks, such as image classification [35, 36], image identification [37] or object detection [38, 39] by feeding. The network with a huge number of images, deep CNNs is proposed to use in the detection and localization of copy-move forgeries in the feature extraction step. AlexNet [40], GoogLeNet [41], ResNet [42], OverFeat [43], VGG-16/VGG-19[33] are some of the most popular CNNs presented in the literature. CNNs are generally designed for three-layer types: convolutional layers, pooling layers, and fully connected layers and train on a huge dataset. Training of an architecture that can be designed to solve considering problems, must train on a huge dataset to obtain efficient results. Because the existing CMFD datasets are inadequate to train a deep neural network, and existing trained deep neural networks have been trained on labeled datasets such as ImageNet [44]. The images in this data set are also suitable for the considered problems.

One of the pre-trained architectures, VGG16 is very preferable due to its very uniform architecture that is trained on a million images from the ImageNet database. In the proposed method, this architecture is used to obtain feature vectors. The network has an image input size of 224-by-224, so in the method firstly, the input image is subdivided into 224x224 sized parts, and feature extraction is performed for each part. If the image or subparts are smaller than this size, the padding operation is performed.

The network consists of 13 convolutional (conv) layers and 3 fully connected layers, 3 max-pooling layers and a softmax classification layer. The conv feature maps are produced by convoluting 3*3 filter windows, the obtained feature map sizes double after every time passing max-pooling layers. In Figure 5, it is shown the kernel sizes of considered architecture in the first three conv layers.

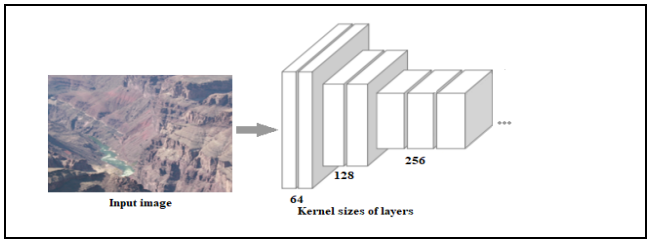


Figure 5. Kernel sizes of convolution layers of used architecture.

In the proposed method to represent each overlapping subblocks the Conv 1-2 layer is used of pretrained VGG16 architecture [33]. The blocks are represented with bxbx64 dimensional features. This mid-level features are selected because of without important information loss and for faster matching.

2.2.2 DCT based feature extraction

DCT has been often preferred to represent the image in the frequency domain because it can represent most of the intensity distribution details by using fewer coefficients. In CMFD methods in the literature, many studies take advantage of this advantage and make the method robust to JPEG attacks.

After the pre-processing phase, let the image forwarded to this stage be I of size, which is split into overlapping squared blocks with a size of 8x8. Each block denoted by is transformed with DCT to the frequency domain. Transformed blocks are zigzag scanned for sorting them from low frequency to high frequency. The coefficients are not quantized by the method to preserve detailed information from smooth regions. The first sixteen elements of the zigzag scanned vector are extracted to obtain feature vectors of each block because low-frequency DCT components are more robust to JPEG compression attacks. The feature matrix is obtained with the feature vectors representing each subblock. Steps of the feature extraction method are given in Algorithm 1 where zigzag() and dct() functions perform zigzag scanning and DCT transformation respectively.

Algorithm 1. DCT based feature extraction

```
Input: Image I
Output: F []

[M, N] =size(I);

for i = 1 to M-8
    for j = 1 to N-8
        b = I(i:i+7, j:j+7);
        f = zigzag(dct(b));
        F [i, j,:] = f (1:16);
    end
end
```

2.2.3 Patch-match based feature matching

In literature, lots of work proved that the dense CMFD techniques have higher performance than keypoint-based ones, with higher execution time problems and being less robust to geometric distortion attacks also. Generally, these disadvantages are caused by the matching stage. In this study, a fast approximate nearest-neighbor search algorithm, Patch Match based method will be used to overcome these problems [32]. While the basic Patch Match algorithm is not robust to rotation and scaling, the method used has been modified to be robust under these attacks.

The Patch Match algorithm is substantially searching for matching offset components (δ_1, δ_2) in 2d space with the generating following steps.

1) Initialization*:* The offset field of each pixel (s) is initialized at random with is a bi-dimensional random variable $U(s)$, $\delta(s) = U(s) - s$. While $\delta(s) = 0$ is discarded, the other candidate offsets are taken which are bigger than a certain threshold for the initial matching to keep the searching space large. Although most of the offsets obtained in the first stage are not good solutions, enough offsets are likely to be enough for the initialization. Because the algorithm aims to generate good solutions rapidly by updating offsets iteratively through the propagation and random search stages,

2) Propagation*:* In this step, for updating the offset $\delta(s)$ of each pixel (s), the image is scanned from top to bottom and left to right with the following condition.

$$\delta(s) = argdis(f(s), f(s + \partial)) \quad (1)$$

Here s^{row} and s^{col} are the previous pixels of (s), on row and columns. Then the scan direction is inverted from bottom to up and right to left at every next iteration. So, through this process, if a good offset is available for the considered pixel of a region, this consistency is rapidly expanded for the whole pixels in the region below and right.

3) Random Search: The quality of the solutions obtained in the previous step highly relies on the solutions obtained in the first stage and maybe achieving a local minimum. To avoid this situation and achieve optimum results, random sampling of the current offset is done.

The original algorithm is not sensitive to scale or rotation changes, to cope with this problem, the authors of [32], a solution to this problem is presented with a simple improvement with searching in 4d space including scale ratio (α) and rotation degree (θ). Further developing this study, in [32], a method that is resistant to these attacks is proposed. It is aimed firstly that the searched patch is rotated and scaled according to the presented degree and ratio, thus becomes corresponding with the original patch. And secondly, in the propagation step, the searching offsets are computed based on the local transformation by scaling ratio and rotation degree.

2.2.4 Post-Processing step

After the matching process is concluded, some falsely matched pixels can appear because the forgery operation can be done with some preprocessing or post-processing attack to hide forgery clues, or the image includes nearly the same regions. Finally, the proposed approach aims to minimize the falsely matched pixels and increase the detection of forged pixels truly. The proposed method aims to detect a forgery in case a copied region is pasted once. For this purpose, the following stages have been realized.

1) Computing the Squared Error of Dense Linear Fitting*;* In lots of CMFD methods, generally RANSAC [46] or SATS [47] algorithms, which are quite complicated and slow, are used to eliminate matches that do not match similar homography. Thanks to Patch Match based matching, there is no need to use such complex algorithms, a dense linear fitting (DLF) based approach is used over a circular neighborhood of radius th_n. After detected regions are formed with a median filter with radius of th_m, the fitting error is calculated and then thresholding with $th = th_m + th_n$. The parameters are set as th_m= 4 and th_n=6 empirically,

2) Removing of Close Couples and Small Regions. The detected forged regions are removed if they are closer than γ_d pixels and if they are smaller than γ_s pixels. (The used parameters are fixed as γ_s=8 and γ_d=50),

3) Applying morphological operations. Finally, morphological opening and dilation operations are implemented to the image to localize the forged pixels better.

3 Experimental results

In this part, it is analyzed the performance of the presented scheme by comparing referenced works. This section is divided

into two subsections, the dataset and evaluation metrics are given at first and concluded with performance evaluation comparison with referenced works. All measurements are performed on a desktop computer with 3.4- GHz Intel Core i7 and 8GB RAM memory, running Matlab 2019(b).

3.1 The dataset and evaluation metrics

Experimental results are realized on the images from the GRIP dataset, which is available online, to make the comparison in a fair manner. The GRIP dataset [32] (www.grip.unina.it) contains 80 colorful images of size 768x1024x3 pixels and the size of the copied regions on the forged images is approximately less than 1% of the image. The dataset accommodates various images with different pattern characteristics such as textured, smooth and mixed. In Figure 6 three forged images are shown obtained from the GRIP to show three different pattern characteristics. Forgery detection becomes harder if the duplicated regions have smooth characteristics similar to the image given in Figure 6(a).

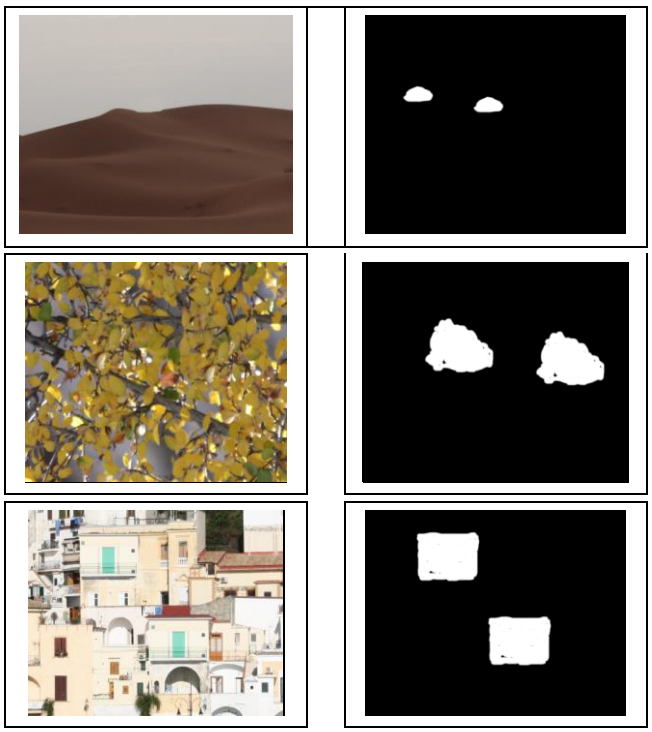


Figure 6. The forgery image examples from the dataset Forged with smooth region, with textured region, with mixed region respectively.

The most challenging problem in the literature is to decrease the detection capability of the CMFD method is even the duplicated regions have smooth characteristics. Various geometric (rotation, scaling, and translation) or image degradation operations can be used to create forged images. If no operation is applied on the forged image after a copy-move operation or no geometric operation is applied before the pasting operation, the resulting attack scenario is called "Plain copy-move forgery". Two other attack types called "Image degradation" and "Geometric distortion" necessitate extra operations during forgery operation. While the former one makes some operations such as white Gaussian noise addition, JPEG compression on the forged image, the latter transforms copied region using rotation, scaling, and translation operations before pasting. Used attack types and parameters in the GRIP dataset are given in Table 1.

Table 1. The number of images with different attacks in the GRIP dataset

Attack Types	Parameter	Range	Step	Num. of Images
JPEG compression	Quality factor	20-100	10	720
Noise addition	Standard deviation	20-100	20	400
Scaling	Scaling factor	91-109	2	800
Rotation	Rotation angle	2-10	2	400

The number of images used for each attack type is also given in Table 1. For testing robustness against JPEG compression attacks, 9x80=720 images are used (Quality factors: 20, 30, …, 100). For noise addition attacks, 5x80=400 images are used (standard deviation: 20, 40, 60, …, 100). For scaling attacks, 10x80=800 images are used. (Scaling factor: 91, 93, 109) For rotation attacks, 5x80=400 images are used. (Rotation angles: 2, 4, ...,10).

Precision, Recall, and F-measure metrics are used to evaluate the performance of the methods that are given in Eq (2). Both image and pixel-level comparisons are realized using these three metrics.

$$Precision = \frac{T_P}{T_P + F_P}, \qquad Recall = \frac{T_P}{T_P + F_N},$$
$$F - measure = 2x\frac{Precision\,.Recall}{Precision + Recall} \tag{2}$$

The meaning of Precision, Recall and F-measure in CMFD evaluations are the same in the work [12]. The higher Precision and Recall ensure a higher F-measure that represents better performance.

3.2 Comparison with the state of the art

In this part, firstly, it is given the average performance of our study and other popular recent works in literature [8],[11],[12],[15],[16],[21],[26],[23],[24]. Zernike moment is chosen as the feature extraction method during getting results of [12], which has the best performance according to authors' reports. Evaluations are done at the pixel level also some evaluations are given at the image level. Average performance results and interpretations are given separately according to attack types applied to forged images. The section is concluded by giving some detected masks of the methods as visual results.

The performance of the proposed method under plain copy-move forgery operation is evaluated first. Plain copy-move forgery is the ideal condition for detection. Table 2 shows the average results of the methods for image-level and pixel-level using F-measure. The worst result for both evaluations is obtained by Christlein2012's approach, which is the SIFT-based method because 40% of the GRIP dataset consists of forged images with smooth regions. Keypoint-based methods will show lower performance with these images because keypoints cannot be obtained from smooth areas. However, the proposed method can label all forged images as forged, but very few original images are mistakenly labeled as forged by the method as can be seen in the results. The proposed scheme shows better performance both at the image and pixel-level

F-measure. For this experiment, 80 plain copy-move images in the dataset were used.

Table 2. Performance outcomes in plain copy-move forgery.

Methods	F-image (%)	F-pixel (%)
Bravo2011	94.12	85.96
Christlein2012	67.72	52.35
Ryu2013	94.63	89.44
Cozzolino2015	94.36	91.67
Li2015	72.13	52.68
Pun2015	95.93	78.11
Zandi2016	86.89	85.10
Bi2017	96.63	96.98
Bi2018	96.63	92.98
Proposed	96.96	97.16

After performance assessment of the methods for plain copy-move forgery detection, firstly the methods are evaluated under scaling attacks. Figure 7 shows the average results of the methods using Precision, Recall, and F-measure metrics respectively. In terms of the Precision metric, the proposed method exceeds the other methods, when we consider the Recall criterion, Bi2017 and Bi2018 are better than others. The proposed method is the best among all the considered methods for all scaling factors when F-measure is considered. According to relevant results, it can be said that more forged pixels can be detected by the proposed scheme with fewer false positives.

We evaluated the suggested scheme under large scaling factors with the methods which share the source codes publicly. The results are obtained forgery images undergone scaling attacks with 0.8 and 1.2 scaling factors. The average F-measure results which are shown in Table 3.

Table 3. The average F- measure results under the scaling attacks with large scaling factors.

Methods	Pixel level (%)		Image level (%)	
	0.8	1.2	0.8	1.2
Bravo2011	2	8	3	68
Christlein2012	0	0	20	11
Cozzolino2015	37	72	68	86
Li2015	48	56	72	74
Zandi2016	2	5	20	15
Proposed	79	89	87	87

It is indicated that the method has the best performance in four evaluations. Although Christlein2012 and Zandi2016 are the key point-based methods, these two studies have yielded almost the worst methods. Since Bravo2011 is a block-based method, it has a low accuracy rate for these situations. The results of the considered methods decline observably, however, the proposed method shows above 79% performance, which points out better performance for both pixel and image-level.

The second experiment gives the experimental results of the rotation attack, which is one of the other geometric degradation attacks. In Figure 8, the obtained results for precision, recall, and f-measure are given with different rotation degrees.

The proposed method has higher performance for precision when compared to other works in the literature. When Recall values are considered, the results of the proposed method are like Cozzolino2015. However, Bi2017 and Bi2018 give higher ratios. The proposed method and the works in Cozzonilo2015, Bi2017, and Bi2018 generate nearly the same results and they have higher f-measures than other methods.

For performance evaluation under image degradation attack, firstly the methods are tested under noise addition attack. The proposed method surpasses other methods in terms of Precision and F-measure metrics. Bravo2011, although the block-based method, shows very low performance, this indicates that this method is not resistant to this attack. In Figure 9 the obtained results are given.

The final experiment was carried out for assessment under JPEG compression attacks. For this observation, the images from the GRIP dataset are Jpeg compressed with 100, 80, 60, 0, 20 quality factors. According to F-measure results, it can be easily noticed that our method outperforms even for quality factor 20. In Figure 10 the obtained results are given.

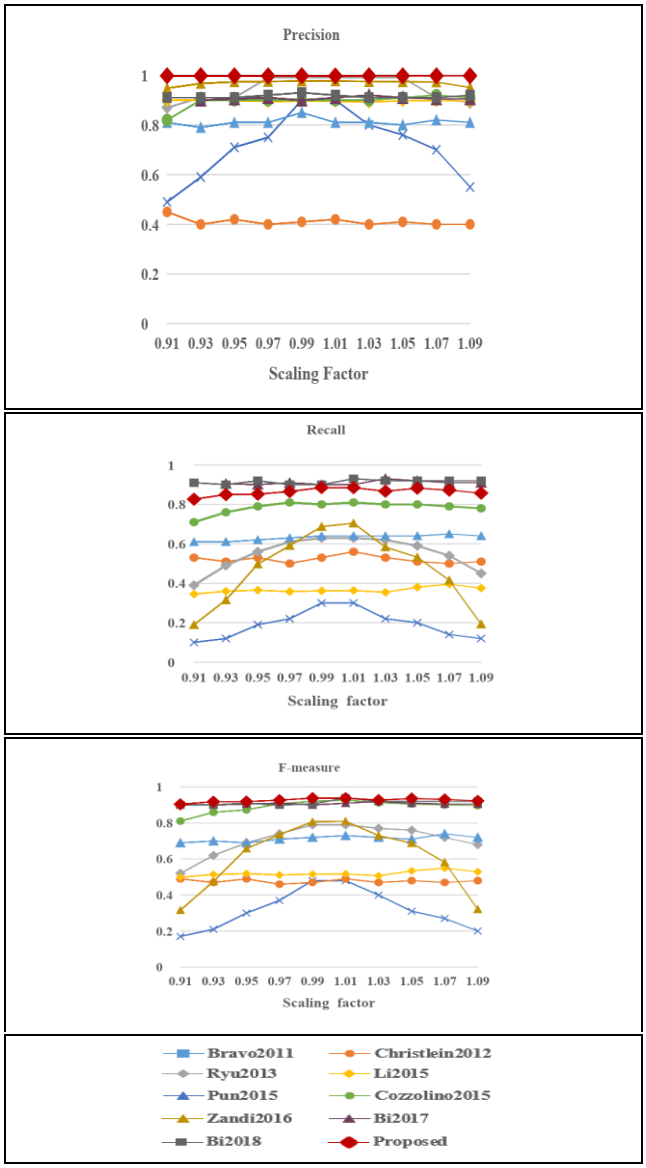


Figure 7. The average results under scaling attacks.

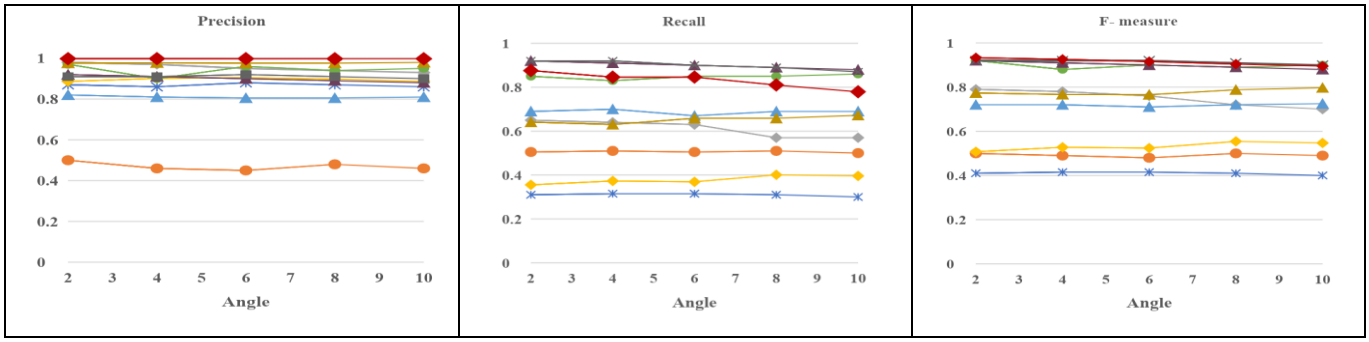


Figure 8. The average results under rotation attacks.

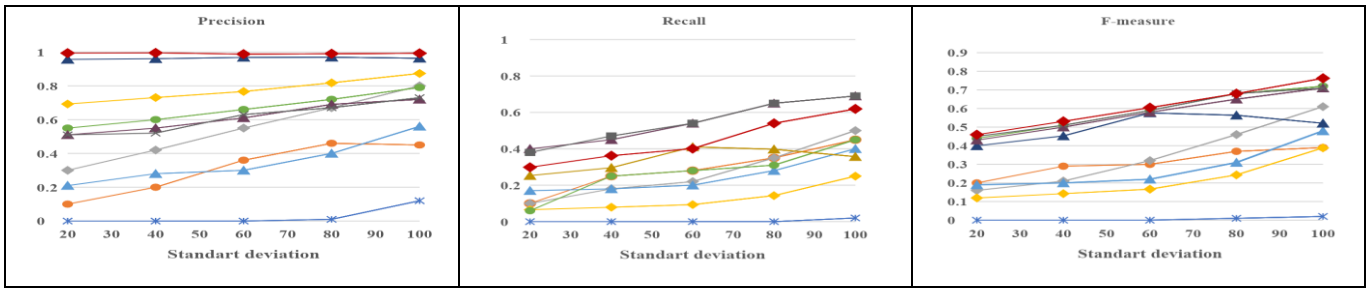


Figure 9. The average result under noise addition attack.

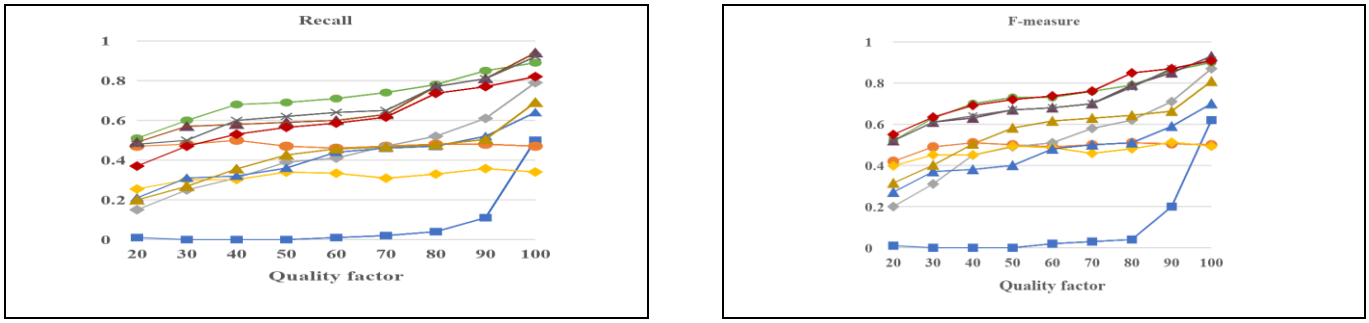


Figure 10. The average result under JPEG compression attack.

This part is concluded by giving some visual results of challenging copy-move forgeries from the GRIP database. The pixels in obtained results are labeled with colors to represent some situations. For this purpose, while correctly detected forged pixels are represented by green color, falsely detected pixels are represented by red color. White color represents forged pixels that cannot be detected by the methods. In this part, to make fair assessments, the comparison is done with Cozzolino2015, Li2015, and Zandi2016, because their source codes were published by the authors. In Figure 11 from top to bottom, the first forgery image is an example of plain copy-move forgery. While Cozzolino2015 and Li2015 cannot detect forgeries, Zandi2016 can detect but the proposed method detects more accurately as can be seen in the figure. This forgery example is done with a smooth region, so the method is the most effective for this challenging situation. In the example given in the second row, the copied region is scaled with 1.2 and then pasted. While Zandi2016 is a keypoint-based method, it cannot detect forged pixels. In the next example, a smooth region is copied and rotated at 8° and then pasted. Li2015 and Zandi2016 fail to detect this forgery. Although Cozzolino2015 detects forged pixels, the method results in a few false positives. Also, for this example, the proposed detects the most accurate result. The first example of the image degradation attack is given in the fourth row, the image has undergone noise with normalized std 0.02. While Zandi2016 cannot detect that the image is forged, Li2015 and Cozzolino2015 produce many false alarms. The forged image given in the last row is an example of the jpeg compression attack with 50 quality factors. Zandi2016 cannot detect forgery regions and also produce some false positives. For this example, the proposed method produces the most effective result.

Table 4 shows the average running time per image on four forged images given in Figure 11. Li2015 is the most time-consuming method because of its EM stage. The method represented with Zandi2016 has shorter working time since it uses parallel pool of Matlab and Cozzolino2015 has shortest running time. Nevertheless, the proposed method achieves has low running time with a better performance than the state-of-the-art methods.

Table 4. The average running times of the methods.

Method	Running Time (s)
Li2015	437
Zandi2016	130
Cozzolino2015	103
Proposed method	110

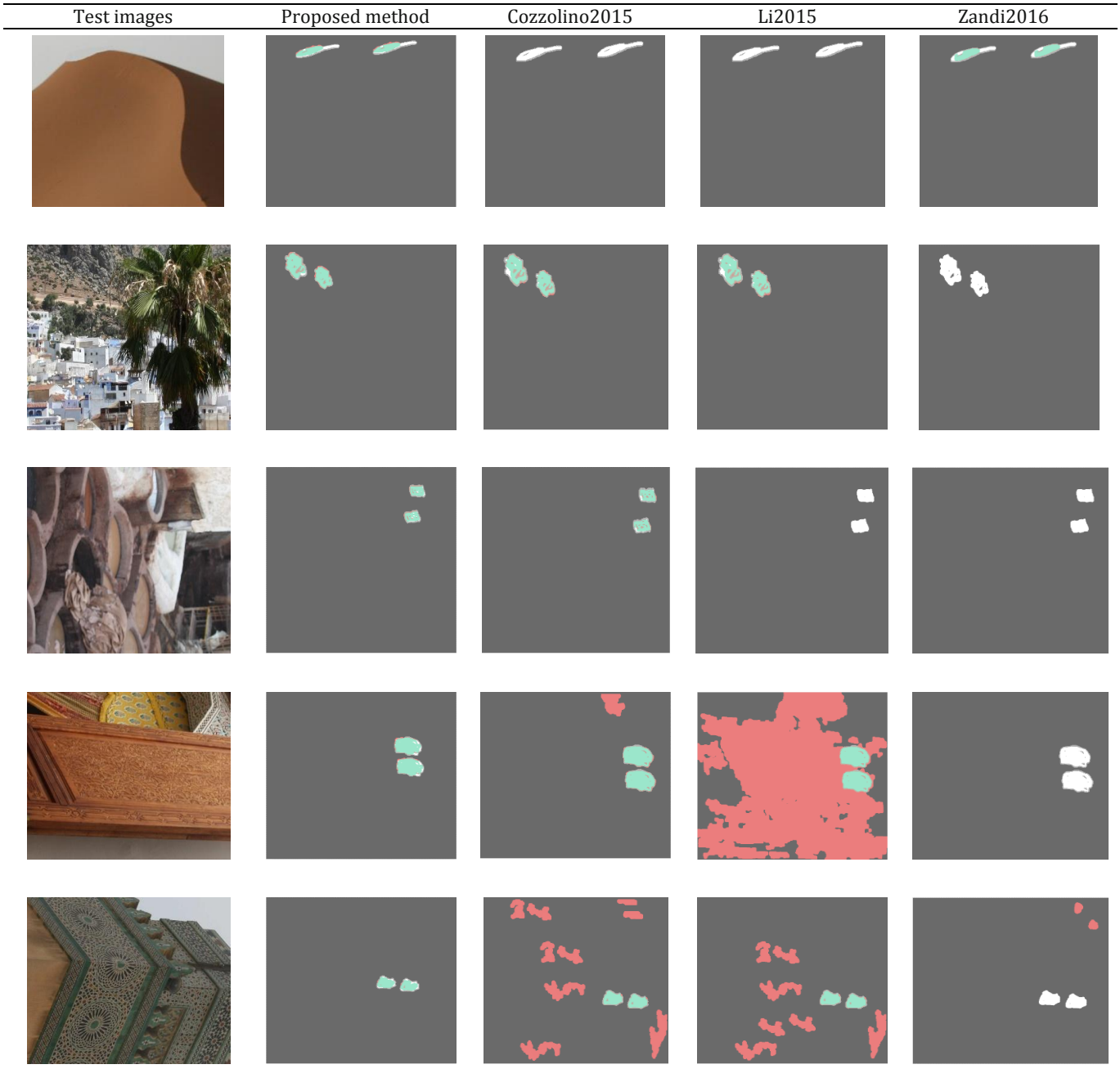


Figure 11. Visual result of forgery detection on some example images of the GRIP database.

As a discussion for weak points of the proposed method, it is failed to detect forgeries under the image degradation attack (such as JPEG compression and noise addition attacks) on the forged images made with smooth regions. In Figure 12 it is given two examples, the first image is undergone JPEG compression attack with 80 quality factors. The forgery could not be detected due to the low contrast information of the duplicated region used in the generalization of the forged image and the distortion of the distinctive information of this region due to the extra attack applied. The second forgery image is undergone noise addition attack with 0.02 standard deviation parameter, the method could not detect this type of forgery also.

4 Conclusion

In this study, it is presented a novel CMFD scheme. The method firstly utilizes the contrast enhancement algorithm based on LDR to obtain more distinct features especially forgeries done with smooth regions. To represent image patches, firstly the feature vectors are obtained from the mid-level of the deep neural network due to their higher performance. The existing trained model is used from a large database as ImageNet, VGG16 for this purpose. Features are obtained from image patches via DCT transformation to make the method more robust against image degradation attacks. Patch Match approach is used to match obtained feature vectors.

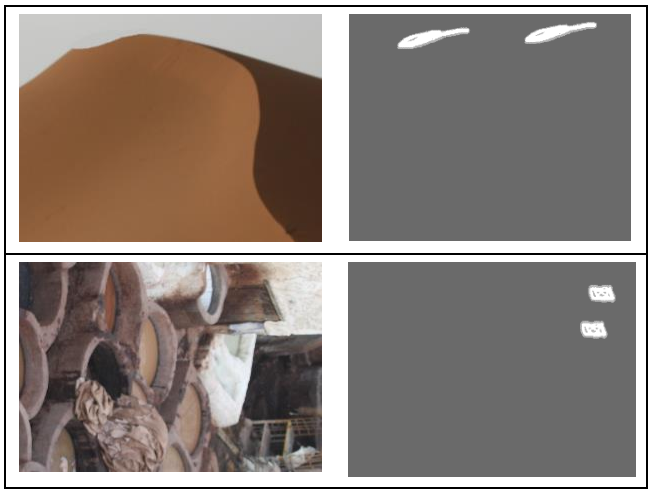


Figure 12. The obtained visual results under image degradation attacks on forged images made with smooth regions.

A specially designed false match elimination step is implemented to minimize false positives after fusing matched regions. When reported experimental results are considered, it can be said that the presented approach has higher performance even when the duplicated region has a smooth characteristic. Results also indicate that the method can successfully detect forgeries even under JPEG compression, noise addition, scaling, and rotation attacks. Our future direction it is planned to design a deep learning network that can be used in the field of copy-paste forgery, enabling more efficient features to be obtained during feature extraction.

5 Acknowledgement

This work was supported by the Scientific and Technological Research Council of Turkey (TUBITAK) with Project No: 119E043.

6 Author contribution statement

Gül TAHAOĞLU contributed to the study under the titles of generating ideas, designing and literature review and the evaluation of the results obtained. Guzin ULUTAŞ contributed to examining the results and checking the article in terms of content.

7 Ethics committee approval and conflict of interest statement

Ethics committee approval is not required for the prepared article. There is no conflict of interest with any person / institution in the prepared article.

8 References

[1] Lian S, Kanellopoulos D. “Recent advances in multimedia information system security”. *Informatica*, 33, 3-24, 2009.

[2] Fridrich A, Soukal JBD, Lukáš AJ. “Detection of copy-move forgery in digital images”. *Digital Forensic Research Workshop*, Ohio, ABD, 6-8 August, 2003.

[3] Popescu A, Farid H. “Exposing Digital Forgeries by Detecting Duplicated Image Regions”. Computer Science Technical Report TR2004-515, 2004.

[4] Mahdian B, Saic S. “Detection of copy-move forgery using a method based on blur moment invariants”. *Forensic Science International*, 171(2-3), 180-189, 2007.

[5] Bayram S, Sencar HT, Memon N. “An efficient and robust method for detecting copy-move forgery”. *IEEE International Conference on Acoustics, Speech and Signal Processing*, New York, USA, 19-24 April 2009.

[6] Luo W, Huang, J, Qiu, G. “Robust detection of region-duplication forgery in digital images”. *International Conference on Pattern Recognition*, Hong Kong, China, 20-24 August 2009.

[7] Wang J, Liu G, Li H, Dai Y, Wang Z. “Detection of image region duplication forgery using model with circle block”. *1st International Conference on Multimedia Information Networking and Security*, Hubei, China, November 2009.

[8] Bravo-Solorio, S, Nandi, AK. “Exposing duplicated regions affected by reflection, rotation and scaling”. *International Conference on Acoustics, Speech and Signal Processing*, Prague, Czech Republic, 22-27 May 2011.

[9] Wu Q, Wang S, Zhang X. "Log-Polar based scheme for revealing duplicated regions in digital images". *IEEE Signal Processing Letters*, 18(10), 559-562, 2011.

[10] Li L, Li S, Zhu H. “An efficient scheme for detecting copy-move forged images by local binary patterns”. *Journal of Information Hiding and Multimedia Signal Processing*, 4(1), 46-56, 2013.

[11] Ryu S, Kirchner M, Lee M, Lee H. “Rotation invariant localization of duplicated image regions based on zernike moments”. *IEEE Transaction on Information Forensics and Security*, 8(8), 1355-1370, 2013.

[12] Cozzolino D, Poggi G, Verdoliva L. “Efficient dense-field copy-move forgery detection”. *IEEE Transactions on Information Forensics and Security*, 10(11), 2284-2297, 2015.

[13] Bi X, Pun C, Yuan X. “Multi-level dense descriptor and hierarchical feature matching for copy-move forgery detection”. *Information Sciences*, 345, 226-242, 2016.

[14] Emam M, Han Q, Niu X, “PCET based copy-move forgery detection in images under geometric transforms”. *Multimedia Tools and Applications*, 75(18), 11513-11527, 2016.

[15] Bi X, Pun CM. “Fast reflective offset-guided searching method for copy-move forgery detection”. *Information Sciences*, 418-419, 531-545, 2017.

[16] Bi X, Pun CM. “Fast copy-move forgery detection using local bidirectional coherency error refinement”. *Pattern Recognition*, 81, 161-175, 2018.

[17] Huang H, Guo W, Zhang Y. “Detection of copy-move forgery in digital images using SIFT algorithm”. *IEEE Pacific-Asia Workshop on Computational Intelligent and Industrial Application*, Wuhan, China, 19-20 December 2008.

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

[19] Amerini I, Ballan L, Caldelli R, Bimbo AD, Del Tongo L, Serra G. “Copy-move forgery detection and localization by means of robust clustering with J-linkage”. *Signal Processing: Image Communication*, 28(6), 659-1669, 2013.

[20] Bo X, Junwen W, Guangjie L, Yuewei D. "Image copy-move forgery detection based on SURF". *International Conference on Multimedia Information Networking and Security*, Nanjing, China, 4-6 November 2010.

[21] Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E. "An evaluation of popular copy-move forgery detection approaches". *IEEE Transactions on Information Forensics and Security*, 7, 1841-1854, 2012.
[22] Zhu Y, Shen X, Chen H. "Copy-Move Forgery Detection Based on Scaled ORB". *Multimedia Tools and Applications*, 75(6) 1-15, 2015.
[23] Li J, Li X, Yang B. "Segmentation-based image copy-move forgery detection scheme". *IEEE Transactions on Information Forensics and Security*, 10(3), 507-518, 2015.
[24] Pun CM, Yuan XC, Li X. "Forgery detection using adaptive oversegmentation and feature point matching". *IEEE Transactions on Information Forensics and Security*, 10 (8), 1705-1716, 2015.
[25] Wenchang S, Fei Z, Bo Q, Bin L. "Improving image copy-move forgery detection with particle swarm optimization techniques". *China Communications*, 13(1), 139-149, 2016.
[26] Zandi M, Mahmoudi-Aznaveh A, Talebpour A. "Iterative copy-move forgery detection based on a new interest point detector". *Transactions on Information Forensics and Security*, 11(11), 2499-2512, 2016.
[27] Yang F, Li J, Lu W, Weng J. "Copy-Move forgery detection based on hybrid features". *Engineering Applications of Artificial Intelligence*, 59, 73-83, 2017.
[28] Li Y, Zhou J. "Image copy-move forgery detection using hierarchical feature point matching". *2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, Jeju, Korea (South), 13-16 December 2016
[29] Rao Y, Ni J. "A deep learning approach to detection of splicing and copy-move forgeries in images". *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, Abu Dhabi, United Arab Emirates, 4-7 December 2016.
[30] Ouyang J, Liu Y, Liao M. "Copy-move forgery detection based on deep learning". *2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, Shanghai, China, 14-16 October 2017.
[31] Yue W, Abd-Almageed W, Natarajan P. "Image copy-move forgery detection via an end-to-end deep neural network". *2018 IEEE Winter Conference on Applications of Computer Vision*, Lake Tahoe, NV, USA, 12-15 March 2018.
[32] Cozzolino D, Poggi G, Verdoliva L. "Copy-move forgery detection based on PatchMatch". *2014 IEEE International Conference on Image Processing (ICIP),* Paris, France, 27-30 October 2014.
[33] Simonyan K, Zisserman A. "Very deep convolutional networks for large-scale image recognition". *International Conference on Learning Representations*, San Diego, CA, 10 April 2015.
[34] Lee C, Kim C. "Contrast enhancement based on layered difference representation". *IEEE Transactions on Image Processing*, 22(12), 5372-5384, 2013.
[35] Li Q, Cai W, Wang X, Zhou Y, Feng DD, Chen M. "Medical image classification with convolutional neural network". *13th International Conference on Control Automation Robotics & Vision (ICARCV),* Singapore, 10-12 December 2014.
[36] Song X, Feng F, Liu J, Li Z, Nie L, Ma J. "Neurostylist: neural compatibility modeling for clothing matching". *25th ACM International Conference on Multimedia*, New York, United States, 23-27 October 2017.
[37] Wu JD, Ye SH. "Driver identification using finger-vein patterns with Radon transform and neural network". *Expert Systems and Application*, 36(3), 5793-5799, 2009.
[38] Erhan D, Szegedy C, Toshev A, Anguelov D. "Scalable object detection using deep neural networks". *Computer Vision Pattern Recognation* (*CVPR)*, 2013. https://doi.org/10.48550/arXiv.1312.2249
[39] Sermanet P, Eigen D, Zhang X, Mathieu M, Fergus R, LeCun Y. "Overfeat: Integrated recognition, localization and detection using convolutional networks". *Computer Vision and Pattern Recognition*, 2014. https://doi.org/10.48550/arXiv.1312.6229
[40] Krizhevsky A, Sutskever I, Geoffrey A, Hinton E. "ImageNet Classification with Deep Convolutional Neural Networks". *Advances in Neural Information Processing Systems*, 2012. https://doi.org/10.48550/arXiv.1409.0575
[41] Szegedy C, Liu W, Jia Y, Sermanet P, Reed S, Anguelov, D, Erhan D, Vanhoucke V, Rabinovich A. "Going Deeper with Convolutions". 2015 *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Boston, MA, USA, 7-12 June 2015.
[42] Jia D, Wei D, Richard S, Li-Jia L, Kai L, Li FF. "Imagenet: A large-scale hierarchical image database". *2009 IEEE Conference on Computer Vision and Pattern Recognition CVPR 2009*, Miami, FL, USA, 20-25 June 2009.
[43] Sermanet P, Eigen D, Zhangm X, Mathieu M, Fergus R, LeCun Y. "Overfeat: Integrated recognition, localization and detection using convolutional networks". *Computer Vision and Pattern Recognition*, 2014. https://doi.org/10.48550/arXiv.1312.6229
[44] Russakovsky O, Deng J, Su H. "ImageNet Large Scale Visual Recognition Challenge". *Computer Vision and Pattern Recognition*, 2015. https://doi.org/10.48550/arXiv.1409.0575
[45] Barnes C, Shechtman E, Finkelstein A, Goldman DB. "PatchMatch: a randomized correspondence algorithm for structural image editing". *ACM Transactions on Graphics*, 28(3), 1-11, 2009.
[46] Fischler MA, Bolles RC. "Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography". *Communications of the ACM*, 24(6), 381-395, 1981.
[47] Christlein V, Riess C, Angelopoulou E. "On rotation invariance in copy-move forgery detection". *IEEE International Workshop Information Forensics Security*, Seattle, WA, USA, 12-15 December 2010.
[48] Ulutas G, Ustubıoglu B, Ulutas M, Nabıyev V. "Video forgery detection method based on local difference binary". *Pamukkale University Journal of Engineering Sciences*, 26(5), 983-992, 2020.
[49] Yang HY, Qi SR, Niu Y, Niu PP, Wang XY. "Copy-Move forgery detection based on adaptive keypoints extraction and matching". *Multimedia Tools and Application*, 78(24), 34585-34612, 2019.
[50] Li Y, Zhou J. "Fast and effective image copy-move forgery detection via hierarchical feature point matching". *IEEE Transactions and Information Forensics Securuty*, 14(5), 1-16, 2019.
[51] Meena KB, Tyagi V. "A copy-move image forgery detection technique based on tetrolet transform". *Journal of Information Security and Applications*, 2020. https://doi.org/10.1016/j.jisa.2020.102481

[52] Wang Y, Kang X, Chen Y. "Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity measures". *Journal of Information Security and Applications*, 2020. https://doi.org/10.1016/j.jisa.2020.102536

[53] Tahaoglu G, Ulutas G, Ustubioglu B, Nabiyev V. "Improved copy-move forgery detection method via L*a*b* color space and enhanced localization technique". *Multimedia Tools Appl*ication, 80, 23419-23456, 2021.

[54] Rodriguez-Ortega Y, Ballesteros DM, Renza D. "Copy-Move forgery detection (CMFD) using deep learning for image and video forensics*". Journal of Imaging*, 2021. https://doi.org/10.3390/jimaging7030059.