Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Tracing Of Identical Key Points For Recognition Of Copy-Move Forgery

Chandrakala[1] , Dr. M Sasikala[2]

[1]Assistant professor GECW.

[2]Principal GECW.

Abstract

Rapid development of digital image processing along with various image editing tools, it is quiet easy to tamper these images without having any traces of modification; hence determining the authenticity of digital image is considered as the social issue. Moreover, several agencies like news services, intelligence service and law firms rely upon the image for various purpose; as a result, variety of researches has been carried out to detect the forgery evidence. Copy Move image forgery (CMF) is most common and popular type of image tampering where regions are selected by attacker and other region are copied into it. Moreover, development of robust and automatic approach for copy move forgery are still considered as an open challenge; thus in this research work, we design and develop an automatic mechanism named TIK-RCMF (Tracing of Identical Key points for Recognition of Copy-Move Forgery). TIK-RCMF tends to obtain the optimal solution in all three steps i.e. extraction of features, similarity matching and tracing of identical points and localization of forgery. In first step, image level optimization is used; in second step optimal similarity checking is utilized and third step optimal localization is achieved. Moreover, performance evaluation is carried out considering the three dataset namely "dataset", "GRIP" and "FAU" considering both image level and pixel level. Furthermore, evaluation is carried out through comparing with different existing mechanism of forgery detection and comparative analysis suggests that TIK-RCMF is efficient than the other models.

Keywords: Copy Move Forgery, TIK-RCMF, key points, similarity checking

1 Introduction

The fast improvement of digital image processing strategies and photo modifying tools, digital images can be without difficulty tampered without leaving glaringly seen lines of any modification [1]-[3]. The accessibility of effective virtual photo process programs, together with Photoshop, makes it notably clean to create virtual forgeries from one or a couple of pics. Therefore, in view,

that pics and their reliability may be seemed as proof or evidence with inside the fields of news, academia, politics, crime investigation, and coverage claims investigation, maliciously forged pics might also additionally convey many substantially destructive issues to society. Copy move image forgery (CMIF)is one of the maximum not unusual place styles of photo tampering, the precept of that's as follows: one or numerous regions (namely, supply regions) are first decided on through an attacker, she or he then copies and pastes them into other regions (namely, goal regions) of the equal photo [4], [5]. To make the forgery appearance extra sensible and convincing, a few extra operations may be carried out to the duplicated regions, together with rotation, scaling, comparison and brightness altering.

Since altered photos are often visually indistinguishable from real images, detecting image forgery has become extremely difficult. A picture can now be manipulated in a variety of ways thanks to high-tech image editing software. Picture manipulation can be divided into two categories: (1) content preservation and (2) content modification [6]. The first form of distortion (compression, blurring, and contrast enhancement) is often caused by post-processing, and it is considered less harmful because it does not affect the semantic content. The latter form (e.g., copy-move, splicing, and object removal) reshapes image content at will and dramatically changes the semantic sense [7]. Manipulation of content can lead to the dissemination of false or misleading facts. As the number of tampered images increases at an exponential pace, it is becoming increasingly important to identify them in order to prevent viewers from being misled. The identification of content-changing alteration from an image or video has recently gained popularity in a variety of science and security/surveillance applications.

Copy Move Forgery is type of forgery where a part of the image is copied and pasted into another part of the same image; this is typically done to render an object “disappear” from an image by covering it with a section copied from another part of the image. Textured areas, such as grass, trees, dirt, or cloth with irregular patterns, are perfect for this since the copied areas would possibly blend in with the context, making any suspicious objects difficult to spot. Since the copied parts are from the same image, their noise variable, colour palette, dynamic range, and most other important properties will be consistent with the rest of the image, and thus will not be observable by methods that search for statistical incompatibilities in different parts of the image. Using the feathered crop or the retouch tool to further obscure any signs of the copied-and-moved segments, making the forgery even more difficult to detect. Any Copy-Move forgery adds a connection between the original and pasted image segments. This connection can be used as a foundation for detecting this form of forgery successfully [8]- [9]. The segments do not fit perfectly but only roughly because the forgery would most likely be saved in the lossy JPEG format and because the retouch tool or other regional image processing software may be used [10]. As a result, the following criteria for the detection algorithm can be formulated first is the detection algorithm should allow for a close match between small image segments, second is It must work in a reasonable amount of time while causing few false positives (i.e., detecting incorrect matching

areas). Another reasonable assumption is that the forged section would be a linked part rather than a series of very small patches or individual pixels.

1.1 Motivation and contribution of research work

In the present era of digital world, digital data images are the main cause of information and it is the best way of conveying knowledge. For the purpose of evidence in courtrooms, the digital image maybe helpful. Since powerful image processing and editing software is readily available, digital images are simple to manipulate and edit. It is now possible to tamper with an image and add or delete essential features without leaving any visible signs of tampering. The need for authenticating digital images, validating their content, and detecting forgeries will only grow as digital cameras and video cameras replace their analogue counterparts. Further, research contribution is highlighted through below points:

1. In this paper, an automatic approach TIK-RCMF is proposed for forgery detection considering the copy move forgery issue; TIK-RCMF tends to achieve the optimal solution for three step i.e. feature extraction, similarity checking and localization of forgery.
2. In feature extraction, contrast optimization and image scaling is carried out for extracting the SIFT key points, for small and smooth regions; in case of second step similarity checking is carried out which solves the key point matching issue. In third step, optimal localization is carried out through iterative approach for model robustness.
3. Performance evaluation is carried out on three standard datasets that comprises the genuine and tampered image; in order to test the robustsness of model image level and pixel level metrics are computed.
4. Furthermore, metrics comparison is carried out with the different model; comparative analysis suggest that other model fails to compute the various metrices excepts

2 Related Work

In image forensics, forgery detection is a hot topic, with a wide body of literature on the subject. Furthermore, since forgery detection and localization are intertwined, all tasks must be considered. Indeed, sliding-window analysis may be used for localization, and localization methods can enable detection with appropriate post-processing. As a result, in order to keep the scale of the study manageable, we will look at it from a historical perspective.

For image forgery analysis, researchers have established a range of heuristic and hand-derived features [8], [12]–[16]; recently, research has shown that deep learning-based approaches can boost forgery detection and localization efficiency [17]. Deep learning systems were equipped to localize image areas with double JPEG compression artefacts suggestive of tampering in [18]-[20]; further[21] created a multi-task completely convolutional network that enhanced forgery localization by training a branch to learn spliced area boundaries. [22] Suggested an LSTM architecture for learning the splice-pristine zone boundary change. A completely convolutional network was also proposed in [23], but it was trained on a specific set of 385 manipulations. The deep-learning-based techniques described above are trained to recognize a specific collection of

forgery features. Techniques that detect anomalies in forensic features [16], [24], and in particular features related to image source [26]- [30], have recently been discovered to be even more effective. Since training a system on all conceivable and real-world manipulations is impossible, instead, these systems look for irregularities and anomalies in forensic features that indicate splicing. a convolutional neural network (CNN) to create deep-feature representations of an image's source camera-model, and then used an iterative k-means clustering approach to detect and localize image forgeries [26]. Following that, we demonstrated in [29] that the similarity of camera-model linked forensic traces could be directly calculated using a CNN-based Siamese network, which can be used to detect image forgeries. research in [24] refined this concept by proposing a more systematic definition of Forensic Similarity, which is a quantifiable measure of similarity of forensic traces linked to the source and/or processing between two image patches, as well as improving the Siamese network technique. [27], [28] proposed a CNN that transforms an image to highlight objects associated with camera-specific traces in their deep learning forensics research. The forged regions were identified by looking for inconsistencies in the resulting fingerprint chart. Huh et al. produced a "consistency map" for forged images using a deep-learning technique [27]. In this consistency map approach, regions of the image that contain EXIF-based metadata predictions that are inconsistent with the rest of the image are highlighted. Huh et al. demonstrated that forgery detection could be performed by taking a spatial average of the consistency map and comparing it to a threshold. The distinction between forgery detection and forgery localization is clearly drawn in multimedia forensics techniques [26], [27]. Forgery detection methods decide whether an image has been tampered with or is otherwise unaltered. Forgery localization methods decide which regions of an image have been tampered with given a forged image.

In [30], an approach was introduced to recognize forgery of copy-move method. DCT (Discrete-Cosine-Transformation) of the picture chunks was utilized and their lexicographical ordering was used to prevent the computational load. The disadvantage of this approach is that it cannot recognize copied regions that are very small. In [31], author introduced algorithm of recognition of duplicate region based on enhanced DCT and shows less complexity in computation. The pointed out variance between this technique and the other techniques that are based on DCT is that here with circle block, the characterization of quantized block is done. However, its performance is bad with the bad quality of the image. It is not accurate with the operations of geometric also. In [32], the researchers introduced an accurate technique to recognize CMF (copy-move forgery) using SVD and DCT. The image is separated into unchangeable size corresponding blocks and 2-dimensional DCT is used to every single block. Then the quantization of coefficient of DCT is done to get more accurate representation of every single block along with separating those quantized blocks into un-corresponding sub-blocks.
Although there has been plethora of work in copy move forgery detection, it is to be noted that in case of CMF, contrast of genuine region and tampered regions are highly consistent which proceeds great challenges

3 Proposed Methodology

In this section of the research, we design and develop TIK-RCMF mechanism for optimal copy-move forgery detection; TIK-RCMF mechanism includes feature extraction, similarity checking and recursive localization. Figure 1 shows the workflow process of TIK-RCMF; it comprises 3 step; first step includes feature extraction which is optimized through image level optimization, second step follows the similarity checking and third step follows the recursive localization; each step and their mathematical formulation has been carried out further

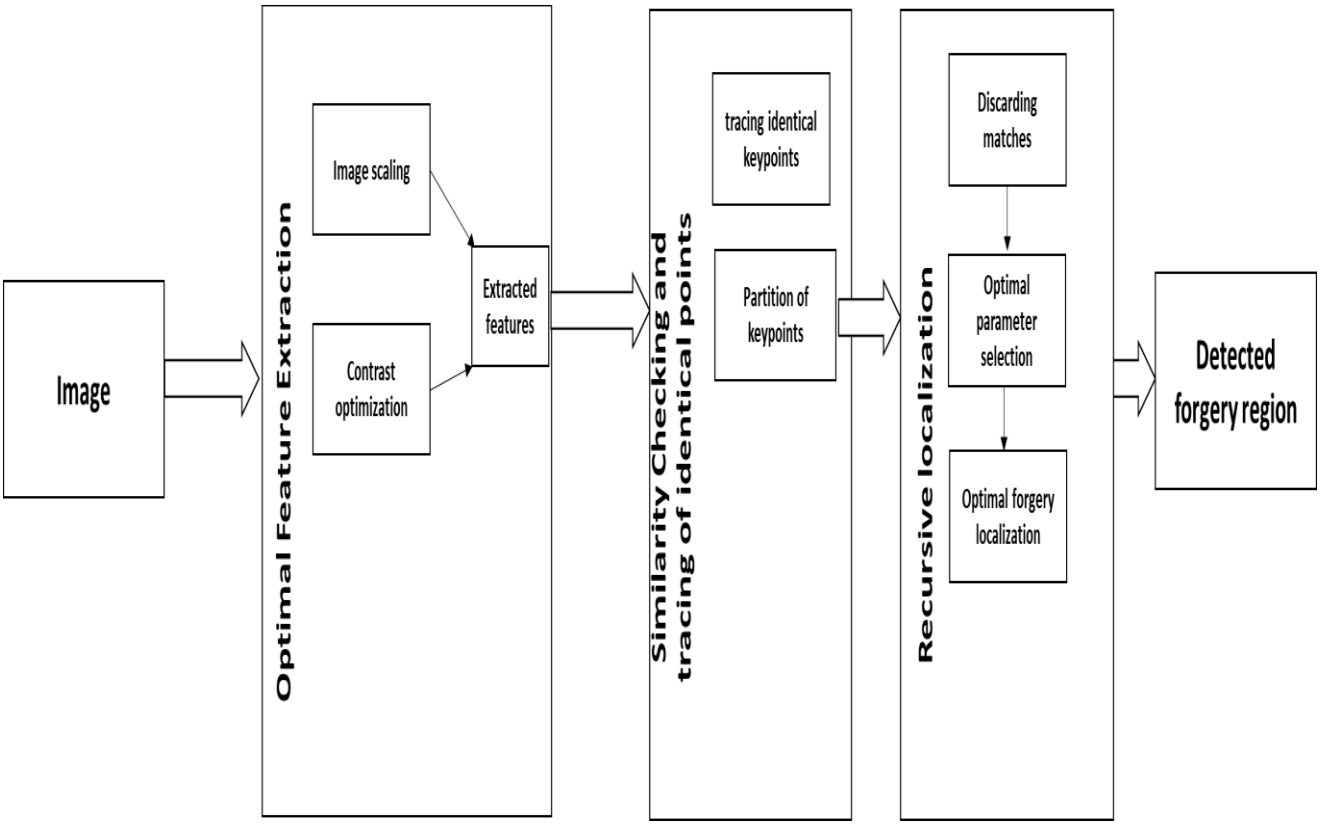

Figure 1 TIK-RCMF workflow process

3.1 Research Preliminaries and feature extraction

The most effective and simple technique for extraction of key point features is SIFT, which is best for transformation of geometric and distortion of noise. In this section, we study about the extraction and matching the key point-features using SIFT technique.

3.1.1 feature design through SIFT feature

The SIFT technique is classified into four stages:

A. key point recognition of feature via scale distance extrema recognition;
B. filtering of the key point based on edge and contrast threshold
C. allocation of each key points at important positions; and

D. extraction of key point descriptor. At first stage, the key point of features are recognized at various scales.

An input picture denoted as **P,** Gaussian-distorted picture is produced by iteratively processing the input picture with Gaussian-refinement at several scales. After that, the key points are chosen as common extrema inside a cube of parameter ψ domain having an axial length 3. Particularly, the picture of Do G at scale φ is denoted as

$$\psi(y, z, \varphi) = M(y, z, y\varphi) - M(y, z, \varphi) \quad (1)$$

Here, y is a constant the is already defined and $M(y, z, \varphi)$represents the blurred image of Gaussian is evaluated by

$$M(y, z, \varphi) = \zeta(y, z, \varphi) \otimes J(y, z) \quad (2)$$

Where, kernel of Gaussian is denoted as $\zeta(y, z, \varphi)$At second stage, all the features of the keypoints are filtered based on the edge and contrast threshold. This operation is important as refuses the unusable extrema within the SIFT technique. At third stage, allocation of each selected key points at important positions to gain changes in rotation. For every single point (y, z, φ)its position is evaluated as

$$\Theta(y, z, \varphi) = \tan^{-1}\left((e_z)\ (e_y)^{-1}\right) \quad (3)$$

Here, e_z and e_y are the horizontal and vertical gradients at point (y, z, φ). A histogram of the positions are then built by collecting the gradient position detail of points within a common window positioned at the keypoint of the SIFT. The highest in the histogram of the position relates to the main position. At the last stage, a descriptor of 128-dimension is evaluated by encoding the nearby detail in the local region (size of 16×16 within the scale space) positioned at the key points of the SIFT. From the above four stages, a collection of total amount of key points $\left\{key_{points_1}, key_{points_2}, \dots, key_{points_o}\right\}$ and their related descriptors $\{RD_1, RD_2, \dots, RD_{total}\}$ are produced for the provided picture **J**. Let key be a common keypoints of the SIFT that is denoted as a vector of four dimension $key_{points} = \left(\left\{y_{key_{points}}, z_{key_{points}}, \varphi_{key_{points}}, \Theta_{key_{points}}\right\}\right)$; here $\left(y_{key_{points}}, z_{key_{points}}\right)$ are the locations of picture plane, $\Theta_{key_{points}}$ acts as the main position and $\varphi_{key_{points}}$ represents the scale.

3.1.2 Feature matching mechanism

To obtain a better trace of the key point key_{points}, typically calculating the displacements between remaining $(o - 1)$ keypoints with respect to a global threshold would not operate nicely at big sized feature space. Here, the tracing process is performed by calculating the ratio of the nearest distance to the next nearest ones. The concept of it is that for those wrong traces, it will mostly be live many wrong traces with same distances. This is due to the distances evaluated in the big sized feature space. Particularly, let vector $e = \{e_1, e_2, \dots, e_O\}$ note the distance of Euclidean among keypoint key and left over key points $(O - 1)$ in an ascending manner. i.e. $e_1 \leq e_2 \leq \cdots \leq e_{O-1}$.

Then, the keypoint key is traced with anyone among the leftover $(\text{total} - 1)$ keypoints only if $m > e_1/e_2$. Here, $m \in (0,1)$ is already assigned.

3.1. Extraction of the Features:

In this section of the paper, we implement a new technique for recognizing the copy-move forgery of the picture for complete and wide feature sets of the picture with the help of SIFT technique for feature extraction. There are total three layers for recognizing whether the given picture is forgery picture or not, 1) Extraction of the Features, 2) Tracing of Feature points, and 3) Localization of Forgery Repetitively, which are explained below: Here, the extraction of the key point features is performed in this section. We are using SIFT technique for extraction of the features as it is best in transformation of geometric and distortion of the noise. As we know that, the main issue for extraction of features based on key point selection is that it cannot extract enough amount of key point features in small or soft parts of the image, which causes to poorer recognition performance. Here we will be using two small but very powerful methods to extract enough SIFT features based on key points, also including small and soft parts of the image, known as, i) Contrast optimization and ii) image rescaling

3.1.1. Image level optimization

In this section we optimize the input at image level, this is carried out through contrast optimization and image rescaling. The threshold of the contrast is represented as T, is already defined to refuse those unusable extrema having minimum values of contrast. Usually, for every single point $w = (i, j, \rho)$ in scale space, whose value of contrast is represented as:

$$\psi(\hat{y}) = \left(\left(\frac{\partial \psi}{\partial y}\right)^{U} \times 0.5 * \hat{y}\right) + \psi \quad (4)$$

Here, DoG is represented in Eqn-1 and $\hat{w}$ is filtered position of w within the linear space. Any extrema having lower value of contrast when compared with T is refused to be finalized keypoints of the SIFT technique. Anyways, we observe that in soft areas, the extrema's value of contrast inclined to be very less. Therefore, some of the extrema or none of the extrema are capable of qualifying the contrast filtering test and at last chosen as key points of SIFT. To make sure that enough amount of key points can be produced in soft parts of the image, we perform the reduction of T in the SIFT technique.Image rescaling is another attempt to make the TIK-RCMF more robust as only contrast optimization fails to generate the particular key points; hence image rescaling is carried out before the computation of key points. Moreover image rescaling increases the feature key points.

3.2 Similarity checking and tracing of key points

In case of recognition of copy-move forgery, the process of tracing the feature key points targets to find out the same local parts within the picture. In this section, we are implementing a new technique known as Tracing of feature points.

3.2.1 Using Scale Grouping for Tracing in Group:

Remember that all key points of the SIFT are recognized in scale space. There the Gaussian pictures are clustered by octave (octave is used to process the picture). When reducing T, the recognized keypoints are various scales can be highly grouped. In our research, our aim is to distinguish highly the recognized grouped key points at various scales. Here, we implement to perform the tracing process for every octave of minimum scales individually, whereas combined in several octaves of maximum scales; furthermore, it is carried out in two steps i.e. the amount of key point features are very less in minimum scale octave when compared with maximum scale octaves. second step follows as; In parallel, tracing the key points in maximum-scale octaves gain effectiveness for the attack of resizing at big scale.

Particularly, consider ρ_{key} be the value of scale of key that can be already gained along with evaluating the keypoints of SIFT. The value of scale of 1st-DoG-picture in p-th octave is given as α_p. In our implementation, the feature points are grouped into three parts based on their values of scale that are represented as H_1, H_2, and H_3. Correctly,

$$\begin{aligned} H_1 &= \left\{key_{points_j} \middle| \alpha_1 > \rho_{key_p} \geq \alpha_1, j = 1, \dots, o\right\}, \\ H_2 &= \left\{key_{points_j} \middle| \alpha_2 > \rho_{key_p} \geq \alpha_2, j = 1, \dots o\right\}, \\ H_3 &= \left\{key_{points_j} \middle| \varphi_{key_{points_j}} \geq \alpha_3, j = 1, \dots, o\right\}. \end{aligned} \quad (6)$$

Then, the tracing operation is performed on H_1, H_2, and H_3 individually. Specifically, for 1st and 2nd octaves, we use the tracing operation in every octave individually. Whereas for maximum octaves, we perform it in many octaves in integrative way. While scale grouping, the feature key points in various groups are distinguished. We observe that, the effectiveness of our technique is much better against other existing techniques.

3.2.3. partition of key points for tracing identical points

To get the tracing alternatives of key, the distance vector dist is evaluated for all remaining keypoints within same group (H_1, H_2, and H_3) . Usually, the efficiency reduces when amount of key point increases, so we aim to make our tracing technique efficiently as there is huge amount of key points extracted from feature extraction. Lets consider any vector$[0, 1, \dots, 255]$ into the L distinctive categories having step size asc_1 with overlapped size d_2 where d_1 is greater than d_2, thus, it can be calculated as $M = \left\lceil \frac{255-d1}{d1-d2} \right\rceil + 1$. Furthermore, let's consider some parameter C_p which comprises $D_q = \{D_{q,1}, D_{q,2}, \dots\dots, D_{q,M}\}, q \in \{1, 2, 3\}$ where $C_{p,i}$parameter holds the entire keypoints in D_q that has gray values which belongs to given jth sub-level

$$D_{q,j} = \left\{key_{points_k} | b_{j \leq} \mu(key_{points_k}) < c_j, keypoints_k \in D_q\right\}, \quad (7)$$

In above equation μ computes the gray scale value that are associated with given keypoints; further it is computed through computing average. Further, we consider $\mathcal{P}_{p,i,}$ as an individual set parameter which contains matched pairs of $c_{p,i}$; further, $\mathcal{P}$ is computed as given

$$Q = \bigcup Q_{q,j} \; q \in \{1,2,3\}, i = 1 \text{ to } M \quad (8)$$

3.3 Recursive localization approach

Forgery localization is a mechanism which identifies the duplicate region in provided in dense fields, thus in this section we utilize recursive localization approach for forgery localization; further the sub steps are given below.

3.3.1 Discarding the matched pairs

In case of copy move forgery mechanism, it is known fact that forgery is carried out through contiguous shape without knowledge, this indicates that absolute matched points is not isolated in the local region, thus we tend to discard the isolated pairs(matching). Moreover, in case of matched pairs i.e. $(key_{points}, \overrightarrow{key_{points}}) \in Q$; let's consider the two distinctive parameter O_l and $\overrightarrow{O_l}$ with location distance as key_{points} and $\overrightarrow{key_{points}}$which is smaller than the designed threshold; further matched pairs are removed through satisfying the below equation.

$$\text{maxim}\{\overrightarrow{O_l}, O_l\} \geq O_\iota, \quad (9)$$

In the above equation, O_ι is considered as two; further we introduce a set parameter N which comprises the remaining matched pairs and formulated as:

$$N = \{(key_{points}, \overrightarrow{key_{points}}) | \max\{\overrightarrow{O_l}, O_l\} O_\iota; \; (key_{points}, \overrightarrow{key_{points}}) \in Q\} \quad (10)$$

3.3.2 Parameter estimation

In the above steps, affine matrix is used for estimation which uses only limited matched pairs from given two regions. Thus, at first the matched pair is chosen; thus considering the parameter $D_{key_{points}}$ and $D_{\overrightarrow{key_{points}}}$ matched key points are observed that are nearer to the key_{points} and $\overrightarrow{key_{points}}$ with $\mathcal{M}_{keys}$ comprising the matched key points in Mand given as:

$$D_{key_{points}} = \{q | \forall q \in N_{keys}, \eta(p,k) < T_d\},$$
$$D_{\overrightarrow{key_{points}}} = \{q | \forall q \in N_{keys}, \eta(p,k') < T_d\} \quad (11)$$

Also, T_d indicates the user set threshold parameter along with η() as the Euclidean distance in place;

$$N_{keys} = \left\{ key_{points} \middle| \exists \overrightarrow{key_{points}}, s.t \left(key_{points}, \overrightarrow{key_{points}} \right) \in N \right\} \quad (12)$$

further another set is computed that comprises the matched pairs and given as:

$$N_l = \left\{ < key_{points}, \overrightarrow{key_{points}} > \middle| key_{points} \in D_l \wedge \overrightarrow{key_{points}} \in D_{l'}; \left(key_{points}, \overrightarrow{key_{points}} \right) \in N \right\}. \quad (13)$$

3.3.3 Parameter selection through image rotation

In order to improvise the estimation, we introduce a dominant orientation approach that is associated with each key points; let's consider a parameter Θ_l for key point key_{points} that can be obtained through the SIFT operation in Furthermore, homography parameter denoted as I_l and formulated as:

$$I_l = \begin{bmatrix} B & u \\ 0^T & 1 \end{bmatrix}, \quad (14)$$

In above equation, t is transition vector and $u = [u_y, u_z]^U$ with B as the non-singular matrix; this matrix is decomposed through below equation where right and left singular vectors denoted as v and u

$$B = \mathbb{A}\mathbb{B}\mathbb{C}^U = (\mathbb{A}\mathbb{C})^T (\mathbb{C}\mathbb{B}\mathbb{C}^U) = S(\Theta_I)\, S(-\Lambda_I)\mathbb{B}S(\Lambda_I), \quad (15)$$

Also, $\mathbb{B}$ indicating factor parameter computed as:$\mathbb{B} = \mathrm{diag}(\omega_1, \omega_2)$; furthermore, rotation parameter can be computed with distinctive parameter Θ_I

$$S(\Theta_I) = \begin{bmatrix} \cos(\Theta_I) & -\sin(\Theta_I) \\ \sin(\Theta_I) & \cos(\Theta_I) \end{bmatrix} = (\mathbb{B}\mathbb{C})^U. \quad (16)$$

Furthermore, copy move patches are capable of being rotated in both directions as anticlockwise and clockwise; moreover, in order to maintain the consistency Θ_I value is mapped in the given range of 0 to 2π which are computed through below equation.

$$\Theta_I = \begin{cases} \cos^{-1}(S_{11}), & \text{if } S_{11} \geq 0 \wedge S_{21} \geq 0 \\ & \text{or } S_{11} < 0 \wedge S_{21} > 0 \\ & \text{if } S_{11} \leq 0 \wedge S_{21} \leq 0 \\ 2\pi - \cos^{-1}(S_{11}), & \text{or } S_{11} > 0 \wedge S_{21} < 0 \end{cases} \quad (17)$$

In above equations, it should be noted that $S_{11} = \cos(\Theta_I)$ and $S_{21} = \sin(\Theta_I)$; validation of correctness is estimated through offset among Θ_I and $\overrightarrow{\Theta_{key_{points}}} - \Theta_{key_{points}}$. A function parameter is defined to estimate

$$g(key_{points}, \overrightarrow{key_{points}}, I_l) = |\theta_{k'} - \Theta_I - \Theta_I|. \quad (18)$$

In order to achieve the estimated I_l along with $g(key_{points}, \overrightarrow{key_{points}}, I_l)$ and matched pair has to be zero. Let N_l be the inlier set generated through the proposed algorithm then $g(key_{points}, \overrightarrow{key_{points}}, I_l) \leq U_\Theta, \forall < key_{points}, \overrightarrow{key_{points}} > \in N_l$,has to be satisfied where U_Θ indicates the pre-defined parameter.Once, I_l is estimated accurately then dominant orientation parameter might be used for selecting the inliers with matched pairs. In case of matched pair defined earlier, $\begin{pmatrix} \overrightarrow{y_l} \\ \overrightarrow{z_l} \\ 1 \end{pmatrix} \approx I_l \begin{pmatrix} y_l \\ z_l \\ 1 \end{pmatrix}$ formulate the following equations. Moreover, considering the l key points of four dimensions i.e. $(y_l, z_l, \sigma_l, \Theta_l)$, then M_H is computed through below equation:

$$N_K = \left\{ \begin{matrix} < key_{points}, \overrightarrow{key_{points}} > \\ g(key_{points}, \overrightarrow{key_{points}}, I_l) \leq U_\Theta; (key_{points}, \overrightarrow{key_{points}}) \in N \} \\ \in N \end{matrix}, \right| \left|| I_l l - \vec{I} ||_2^2 < \quad (19)$$

Furthermore, I_l is refined through using the inliers, this can be formulated into the optimization problem as given,

$$\dot{I}_l = \arg\min \sum_{<key_{points}, \overrightarrow{key_{points}}> \in N_K} || I_l l - \vec{I} ||_2^2 \quad (20)$$

3.3.4 Optimal Forgery localization

In this section of the research, we design a novel approach for forgery localization; moreover, this localization approach does not require the clustering or segmentation approach. Furthermore, proposed approach is a dual integrated approach where first sub mechanism suspicious region is constructed considering the inliers and second step is optimization of suspicious regions through validation of color.

First step: At first, proposed model tends to construct the local suspicious region in N_K where radius with the key point is given through below equations where σ_k is denoted as the l scale value along with α hyper parameter.

$s_l = \varrho\varphi_l.$	(21)

Second step: In this step we tend to optimize the regions through adjusting the color information; in case of each point given in S, the color transformation is given as:

$\text{key}_{\text{points}\ *} = \hat{I}_l \text{key}_{\text{points}}, \text{key}_{\text{points}} \in T.$	(22)

In above equation, if k and k_* has the similar color value, then it is considered as the copy move points. Furthermore, let's consider the distinctive color components of RGB with respect to point K which can be denoted as $R(\text{key}_{\text{points}})$, $G(\text{key}_{\text{points}})$ and $B(\text{key}_{\text{points}})$ with Q_1 as a whole point recorder

$R_1 = \{\text{key}_{\text{points}}, \text{key}_{\text{points}\ *} \mid \max\begin{pmatrix} \lvert R(\text{key}_{\text{points}}) - \overline{R(\text{key}_{\text{points}\ *})}\rvert, \lvert G(\text{key}_{\text{points}}) - \overline{G(\text{ke} \\ \left\lvert G(\text{key}_{\text{points}}) - \overline{G(\text{key}_{\text{points}\ *})}\right\rvert \end{pmatrix} < U_{\text{rgb};}\ l \in T\}$	(23)

In the above equation, $\overline{R(\text{key}_{\text{points}})}$ is computed through below equation where $\Omega(\text{key}_{\text{points}})$ is a patch along with Z as the normalization parameter; similarly $\overline{B(\text{key}_{\text{points}})}$ and $\overline{G(\text{key}_{\text{points}})}$ can be computed.

$\overline{R(\text{key}_{\text{points}})} = \frac{1}{\mathbb{A}} \sum_{\text{key}_{\text{points}} \in \Omega(\text{key}_{\text{points}})} R(\text{key}_{\text{points}}),$	(24)

Furthermore, we consider a parameter or given T' and it can be formulated as:

$\overrightarrow{\text{key}_{\text{points}}} = \hat{K}_l^{-1} \overrightarrow{\text{key}_{\text{points}}}, \overrightarrow{\text{key}_{\text{points}}} \in T'.$	(25)

Also, considering S', we compute Q_2

$R_2 = \{\overrightarrow{\text{key}_{\text{points}}}, \overrightarrow{\text{key}_{\text{points}}} *\mid \max\begin{pmatrix} \lvert R(\overrightarrow{\text{key}_{\text{points}}}) - \overline{R(\overrightarrow{\text{key}_{\text{points}}} *)}\rvert, \lvert G(\overrightarrow{\text{key}_{\text{points}}}) - \overline{\left(G(\overrightarrow{\text{key}_{\text{points}}})\right)}\rvert, \\ \left\lvert G(\overrightarrow{\text{key}_{\text{points}}}) - \overline{G(\overrightarrow{\text{key}_{\text{points}}} *)}\right\rvert \end{pmatrix} < U_{\text{rgb};}\ \overrightarrow{\text{key}_{\text{points}}} \in T'\}$	(26)

At last another parameter is assumed denoted as $\mathbf{C}$ for binary map along with similar input image size, meanwhile unit is used as the forged parts and zero is used as the genuine location. Furthermore, parameterB is updated through considering the points R_1 and R_2 and formulated as

$\mathbf{C}(R_1 \cup R_2) = 1.$	(27)

Moreover, once the iterations process is carried out, proposed model is able to generate the forgery regions through the sequential approach as discarding the small regions and filling them with close operation; also an image is considered as real image only if its value reaches to 0 else considered as the forged.

4 Performance Evaluation

In this section of the research, we evaluate the proposed methodologies; moreover, the evaluation is carried out considering the three distinctive dataset i.e. FAU [33], Dataset [34], GRIP [35] which all consist of tampered images and corresponding ground truth images. The images in Dataset [34], GRIP [35] have low resolution with size 1000 × 700 whereas image size of FAU [33] is 3000 × 2000.

4.1 Evaluation metrics

TIK-RCMF is evaluated considering pixel level and image level; at image level focus is on the image ability for classification as the authentic or forged. Furthermore, at pixel level, this research work tends to analyze the tampered region location performance and further it verifies the model robustness. Furthermore, considering the image tampered images or pixels as the positive sample and authentic pixels or image as the negative, performance metrics are computed. Moreover, performance metrics includes F1-Score, TPR (True Positive Rate) and FPR(False Positive rate); TPR depicts the actual tampered images in the detection part also known as the Recall and it is computed through below equation.

$$\mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}$$

Similarly, FPR depicts the total number of images mistaken as the tampering image which should be low; FPR is computed as:

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{TN} + \mathrm{FP}}.$$

Furthermore, in above equations true positive i.e. TP indicates the compromised images classified as compromise image i.e. correct detection whereas False Positive is the authentic images classified as false detection. Similarly, False Negative is the number of compromised pixels or images classified as the authentic whereas true negative is number of compromised pixels or

images classified as the authentic image. F1 is a comprehensive evaluation index, which is regarded as a harmonic average of precision and recall rate. The higher value of F1, the better experimental results can be reflected. TPR, FPR, and F1-image are used at the image level, and F1-pixel is used at the pixel level.

$$F_1 = \frac{2TP}{2TP + FP + FN}.$$

4.2 Comparison mechanism and comparative analysis

Furthermore, TIK-RCMF is evaluated through comparing with the different copy move forgery model i.e. Patch Match [35], Hierarchical matching [36] and Iterative strategy [37]; hierarchical matching is solely based on the SIFT key point. [38] was developed based on iterative based approach considering novel interest point detector; in here procedure is iterate through adjusting the key points density. Moreover, Patch Match is rotation invariant approach which is suited for computation of dense fields; next section focus on data based comparison to prove the model efficiency.

4.2.1 FAU-Dataset comparison

FAU is one of the classical dataset that comprises the 48 images; average size of compromised region is nearly 10% of image; moreover, tampering consists of image scaling, image rotation, noise and JPEG compression

A. Image Level

At first we compare the image level comparison considering the three distinctive parameter i.e. F1-Score, FPR and TPR, the value of comparison with different model is depicted in table 1. Furthermore, it is observed that both existing and proposed model achieves 100% of TPR and F1-Score and 0 FPR in comparison with the other model.

Table 1 Image Level

Methodologies	F1-score	FPR	TPR
Hierarchical	98.97	2.08	100
Iterative	79.35	52.08	100
PM-ZM-Polar	94.95	NA	NA
Existing	100	0	100
Proposed	100	0	100

B. Pixel Level

Table 2 depicts the pixel level comparison considering the metrics as F1-core, precision and recall; furthermore, it is observed that proposed model achieves the 99.46% of F1-score in comparison

with 99.24 % of F1-score of existing model. Similarly, for precision and recall existing model achieves 99.96 % and 98.59 % respectively whereas proposed model achieves 100% for both precision and recall. Figure 2 shows the pictorial comparison of existing and proposed mechanism.

Table 2 Pixel Level

Methodologies	F1-score	Precision	Recall
Hierarchical	94.28	NA	NA
Iterative[]	86.07	NA	NA
PM-ZM-Polar	93.72	NA	NA
Existing	99.24	99.96	98.59
Proposed	99.46	100	100

Figure 2 graphical comparison of different metrics

4.3 GRIP dataset comparison

GRIP dataset comprises 160 images of Ground truth and tampered; in here tampered region acquire the arbitrary shape that ranges its size from 400 to 50000 pixels.

4.3.1 Image Level

Table 3 shows the metrics comparison where TIK-RCMF observed 98.08% of F1-score in comparison with other model; however hierarchical method has 100% of F1-score value. Furthermore, TIK-RCMF observes FPR value of 0.036145; also other mechanism observes higher FPR except Hierarchical which observes 0 FPR. Similarly, in terms of TPR all existing model mentioned performs well with 100% value except existing one with 90%.

Table 3 Image Level

Methodologies	F1-score	FPR	TPR
Hierarchical	100	0	100
Iterative	85.56	33.75	100
PM-ZM-Polar	97.53	6.25	98.75
Existing	91.72	10.42	90.00
Proposed	98.08	0.036145	100

4.3.2 Pixel Level

Table 5 shows the pixel level comparison of various methodologies considering the F1 score, Precision and Recall metrics; in here proposed model observes the 99.72 % in comparison with existing model i.e. 99.72% whereas other model stays with low F1-score. Similarly, in case of precision proposed model achieves 100% precision in comparison with 99.96% of existing model; moreover, other model did not compute precision. Furthermore, TIK-RCMF achieves the recall value of 99.02 in comparison with recall value of 98.59 of existing model. Figure 3 shows the pictorial comparison with the model

Table 4 pixel level

Methodologies	F1-score	Precision	Recall
Hierarchical	94.66	NA	NA
Iterative	66.44	NA	NA
PM-ZM-Polar	96.15	NA	NA
Existing-SNS[38]	99.72	99.96	98.59
Proposed	99.46	100	99.02

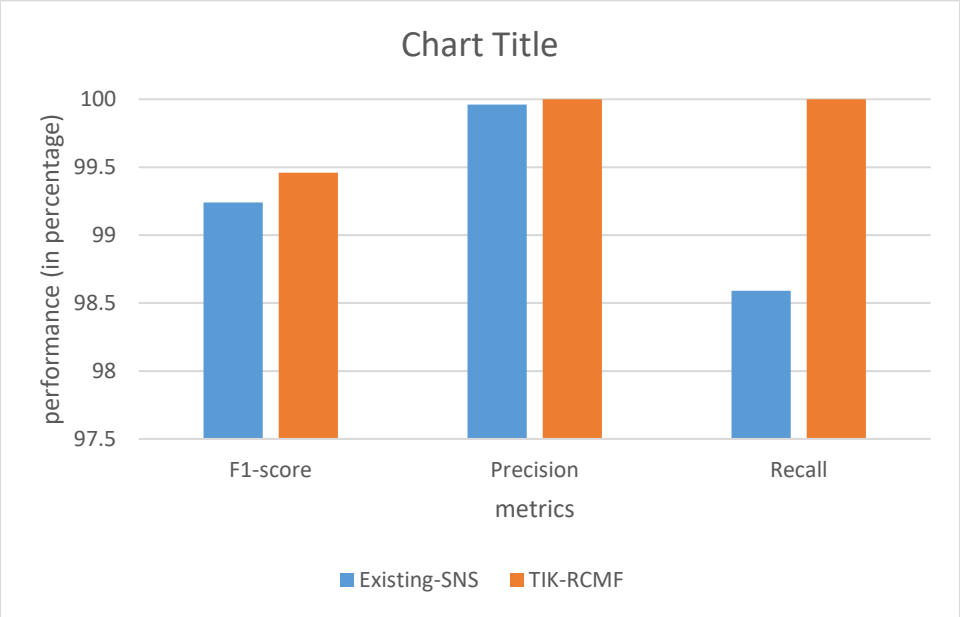

Figure 3 pixel level comparison with the exsting-SNS model

4.4 Dataset comparison

This is another type of dataset named "dataset" which comprises three distinctive parts where D0 consists 50 tampered images; D1 and D2 comprises 20 GOI (Group of Image) with image scaling and rotation. D3 comprises 50 original image.

4.4.1 Image level

Table 5 presents the metrics comparison with various methodologies; in here TIK-RCMF observes F1-score of 98.99 % in comparison with 93.75% and other model observed further F1-score. Similarly, in case of FPR metrics, TIK-RCMF observed the lowest value of 0.019608 in comparison with others. Furthermore, in case of TPR metrics, TIK-RCMF achieves the 100% TPR in comparison with the other mechanism.

Table 5 image level comparison

Methodologies	F1-score	FPR	TPR
Hierarchical	98.00	2	98.00
Iterative[]	84.75	36.00	100
PM-ZM-Polar	96.97	2.00	96.00
Existing-SNS[38]	93.75	2.00	90.00
Proposed	98.99	0.019608	100.00

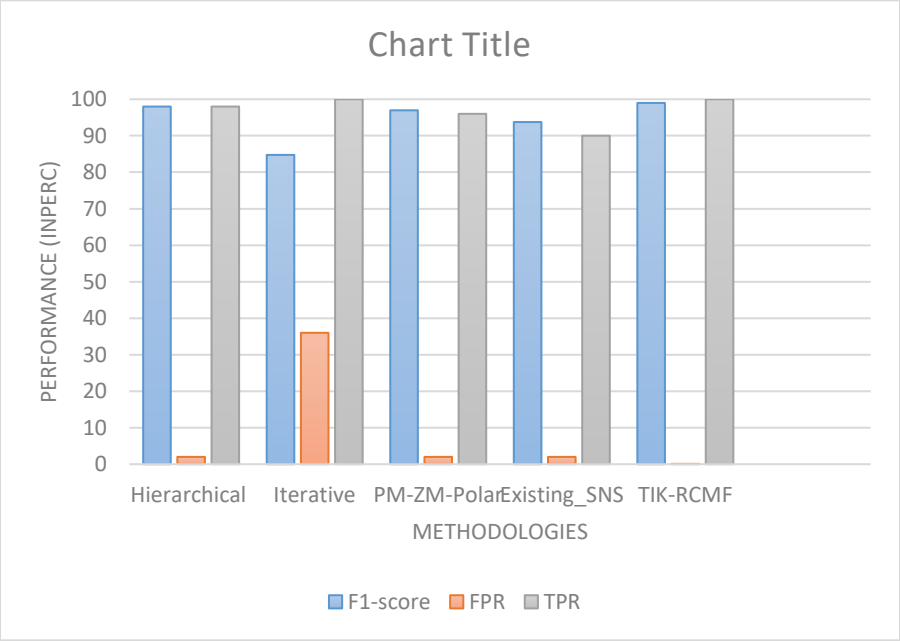

Figure 4 image level comparison

4.4.2 Pixel Level

Table 6 shows the pixel based comparison considering "dataset" dataset, TIK-RCMF observes F1-score of 96.62% whereas existing model achieves 98.07% whereas other model is observing further lower F1-score than other model. Similarly, TIK-RCMF achieves 100% precision in comparison with 99.58 % of existing model; furthermore, TIK-RCMF achieves 94.15 % in comparison with existing model value of 98.07%.

Table 6 pixel level comparison

Methodologies	F1-score	Precision	Recall
Hierarchical	91.45	88.36	91.45
Iterative	81.40	73.52	81.40
PM-ZM-Polar	93.33	89.02	93.33
Existing	98.07	99.58	98.07
Proposed	96.62	100	94.15

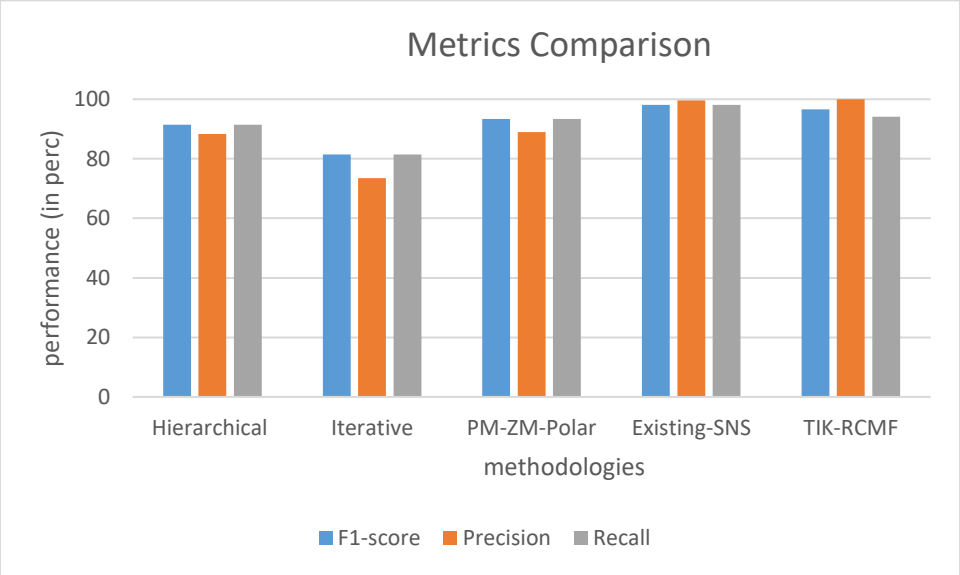

Figure 5pixel level comparison considering different metrics

Conclusion

Copy Move forgery detection aka CMFD is a classical process of identifying the presence of copied region in a given image; moreover, key point based CMFD is one of the efficient mechanism to solve issue of CMF (Copy Move Forgery). Hence, in this research work, we design and develop TIK-RCMF approach for similarity checking of key points; TIK-RCMF comprises three state mechanism i.e. feature extraction, image optimization and optimal forgery localization. TIK-RCMF approach follows the optimal way in each step. Moreover, TIK-RCMF is evaluated considering the standard dataset like "dataset", "GRIP" and "FAU" considering the image level and pixel level evaluation for enhanced evaluation. Furthermore, these datasets are evaluated considering the performance metrics like TPR, FPR and F1-score and recall for image level; also F1-score, precision and recall are computed for pixel level. Further evaluation is carried out through comparing with the various existing methodologies, moreover comparative analysis suggests that proposed methods achieves nearer to the 100% performance in all metrices.

Although, TIK-RCMF simply outperforms the other methodologies till the research has been carried out, it is to be noted that in case of CMF, contrast of genuine region and tampered regions are highly consistent which proceeds great challenges; thus in future, TIK-RCMF can be evaluated with more dataset along with the different image size.

Reference

1. M. C. Stamm, Min Wu, and K. J. R. Liu, "Information forensics: an overview of the first decade," IEEE Access, vol. 1, pp. 167–200, 2013.
2. F. Peng, L. Yin, L. Zhang, and M. Long, "CGR-GAN: CG facial image regeneration for anti-forensics based on generative adversarial network," IEEE Trans. Multimed., 2019.

3. Kakar P, Sudha N, and Ser W, “Exposing digital image forgeries by detecting discrepancies in motion blur,” IEEE Trans. Multimed., vol. 13, no. 3, pp. 443-452, 2011.
4. Y. Li and J. Zhou, “Fast and effective image copy-move forgery detection via hierarchical feature point matching,” IEEE Trans. Inf. Foren. Secur., vol. 14, no. 5, pp. 1307–1322, May. 2019.
5. M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour, “Iterative copy-move forgery detection based on a new interest point detector,” IEEE Trans. Inf. Foren. Secur., vol. 11, no. 11, pp. 2499–2512, 2016.
6. B. Chen, W. Tan, G. Coatrieux, Y. Zheng and Y. Q. Shi, "A serial image copy-move forgery localization scheme with source/target distinguishment," in IEEE Transactions on Multimedia, doi: 10.1109/TMM.2020.3026868.
7. J. H. Bappy, C. Simons, L. Nataraj, “Hybrid LSTM and Encoder– Decoder Architecture for Detection of Image Forgeries,” IEEE Trans. Image Process., vol. 28, no. 7, pp. 3286-3300, 2019.
8. Y. Zhu, C. Chen, G. Yan, Y. Guo and Y. Dong, "AR-Net: Adaptive Attention and Residual Refinement Network for Copy-Move Forgery Detection," in IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6714-6723, Oct. 2020, doi: 10.1109/TII.2020.2982705.
9. C. Wang, Z. Zhang, Q. Li and X. Zhou, "An Image Copy-Move Forgery Detection Method Based on SURF and PCET," in IEEE Access, vol. 7, pp. 170032-170047, 2019, doi: 10.1109/ACCESS.2019.2955308.
10. E. A. Armas Vega, E. González Fernández, A. L. Sandoval Orozco and L. J. García Villalba, "Passive Image Forgery Detection Based on the Demosaicing Algorithm and JPEG Compression," in IEEE Access, vol. 8, pp. 11815-11823, 2020, doi: 10.1109/ACCESS.2020.2964516.
11. F. Matern, C. Riess, and M. Stamminger, “Gradient-based illumination description for image forgery detection,” IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 1303–1317, 2020.
12. M. K. Johnson and H. Farid, “Exposing digital forgeries through chromatic aberration,” in Proc. 8th Workshop Multimedia Secur., 2006, pp. 48–55.
13. O. Mayer and M. C. Stamm, “Accurate and efficient image forgery detection using lateral chromatic aberration,” IEEE Trans. Inf. Forensics Secur., vol. 13, no. 7, pp. 1762–1777, Jul. 2018.
14. J. Lukáš, J. Fridrich, and M. Goljan, “Detecting digital image forgeries using sensor pattern noise,” in Proc. Electron. Imag. Int. Soc. Opt. Photon., 2006, pp. 60 720Y–60 720Y.
15. M. Chen, J. Fridrich, J. Lukáš, and M. Goljan, “Imaging sensor noise as digital X-Ray for revealing forgeries,” in Proc. Int. Conf. Inf. Hiding, 2007, pp. 342–358.
16. D. Cozzolino, G. Poggi, and L. Verdoliva, “Splice buster: A new blind image splicing detector,” in Proc. Int. Workshop Inf. Forensics Secur., 2015, pp. 1–6.
17. L. Verdoliva, “Media forensics and deepfakes: An overview,” 2020, arXiv:2001.06564.

18. M. Barni et al., "Aligned and non-aligned double JPEG detection using convolutional neural networks," J. Vis. Commun. Image Representation, vol. 49, pp. 153–163, 2017.
19. I. Amerini, T. Uricchio, L. Ballan, and R. Caldelli, "Localization of JPEG double compression through multi-domain convolutional neural networks," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops, 2017, pp. 1865–1871.
20. Q. Wang and R. Zhang, "Double JPEG compression forensics based on a convolutional neural network," EURASIP J. Inf. Secur., vol. 2016, no. 1, pp. 1–12, 2016.
21. R. Salloum, Y. Ren, and C.-C. J. Kuo, "Image splicing localization using a multi-task fully convolutional network (MFCN)," J. Vis. Commun. Image Representation, vol. 51, pp. 201–209, 2018.
22. J. H. Bappy, C. Simons, L. Nataraj, B. Manjunath, and A. K. Roy Chowdhury, "Hybrid LSTM and encoder–decoder architecture for detection of image forgeries," IEEE Trans. Image Process., vol. 28, no. 7, pp. 3286–3300, Jul. 2019.
23. Y. Wu, W. Abd Almageed, and P. Natarajan, "Mantra-net: Manipulation tracing network for detection and localization of image forgeries with anomalous features," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2019, pp. 9543–9552.
24. O. Mayer and M. C. Stamm, "Forensic similarity for digital images," IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 1331–1346, Jun. 2020.
25. L. Bondi, S. Lameri, D. Gera, P. Bestagini, E. J. Delp, and S. Tubaro, "Tampering detection and localization through clustering of camera-based CNN features," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops, 2017, pp. 1855–1864.
26. M. Huh, A. Liu, A. Owens, and A. A. Efros, "Fighting fake news: Image splice detection via learned self-consistency," in Proc. 5th Eur. Conf. Comput. Vis., 2018, pp. 101–117.
27. D. Cozzolino and L. Verdoliva, "Camera-based image forgery localization using convolutional neural networks," in Proc. 26th Eur. Signal Process. Conf., 2018, pp. 1372–1376.
28. D. Cozzolino and L. Verdoliva, "Noiseprint: A CNN-based camera model fingerprint," IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 144–159, May 2020.
29. O. Mayer and M. C. Stamm, "Learned forensic source similarity for unknown camera models," in Proc. Int. Conf. Acoust., Speech Signal Process., 2018, pp. 2012–2016.
30. Fridrich, J. Soukal, D. Luk, J. (2003), "Detection of copy-move forgery in digital images", Proc. Digital Forensic Research Workshop, Cleveland, OH, USA.
31. Cao, Y. Gao, T. Fan, L. Yang, Q. (2012), "A Robust Detection Algorithm For Copy-Move Forgery in Digital Images", Forensic Science International, vol. 214, No. 1–3, pp. 33–43.
32. Zhao, J. and Guo, J. (2013), "Passive Forensics For Copy-Move Image Forgery Using A Method Based On DCT And SVD", Forensic Science International, Vol. 233, pp. 158–166.

33. [V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, ‘‘An evaluation of popular copy-move forgery detection approaches,’’ IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.
34. E. Ardizzone, A. Bruno, and G. Mazzola, ‘‘Copy–Move forgery detection by matching triangles of key points,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 10, pp. 2084–2094, Oct. 2015.
35. D. Cozzolino, G. Poggi, and L. Verdoliva, ‘‘Efficient dense-field Copy– Move forgery detection,’’ IEEE Trans. Inf. Forensics Secur., vol. 10, no. 11, pp. 2284–2297, Nov. 2015.
36. Y. Li and J. Zhou, ‘‘Fast and effective image copy-move forgery detection via hierarchical feature point matching,’’ IEEE Trans. Inf. Forensics Security, vol. 14, no. 5, pp. 1307–1322, May 201.
37. M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour, ‘‘Iterative copy move forgery detection based on a new interest point detector,’’ IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2499–2512, Nov. 2016,
38. H. Chen, X. Yang and Y. Lyu, "Copy-Move Forgery Detection Based on Key point Clustering and Similar Neighborhood Search Algorithm," in IEEE Access, vol. 8, pp. 36863-36875, 2020, doi: 10.1109/ACCESS.2020.2974804.