IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Efficient Copy-Move Forgery Detection through Identical Key feature Recognition and Tracing (IKFR-T)

Mohan D N[1], Dr S K Yadav[2]
[1]Research Scholar, Department of Computer Science & Engineering, Shri JJT University, Jhunjhunu, Rajasthan, India
[2]Research Guide, Department of Computer Science & Engineering, Shri JJT University, Jhunjhunu, Rajasthan, India

Abstract

The practice of copy-move forgery is prevalent in various industries, where images often serve as crucial graphical evidence that can be manipulated using various methods. While machine intelligence has been employed for detecting forged digital images in recent decades, achieving accurate detection remains a challenging task. This research introduces a novel method, IKFR-T (Identical Key Feature Recognition and Tracing), designed for effective copy-move forgery detection in digital images. The methodology involves three key steps: feature extraction, similarity checking, and recursive localization, each optimized for improved performance. Results and discussions highlight the effectiveness of IKFR-T, demonstrating superior performance compared to existing models. Evaluation metrics, including F1-Score, True Positive Rate (TPR), and False Positive Rate (FPR), emphasize the methodology's reliability in detecting copy-move forgeries. The research employs the GRIP dataset, illustrating its applicability to real-world scenarios and providing insights into potential advancements and challenges in copy-move forgery detection.

Keyword : Copy move forged detection (CMFD), Image Forgery, Key feature, Identical Key feature Recognition and Tracing (IKFR-T)

1 Introduction

In today's digital era, image authentication faces significant challenges due to the widespread availability of powerful and user-friendly image editing tools, making the identification of original images a daunting task. The internet is flooded with billions of digital photos, many of which undergo digital manipulation, leading to issues like image tampering, copy-move forgery (CMF), and other image manipulations. Such manipulations are prevalent across various fields, including medical imaging, journalism, digital cinema, and special effects in films. Detecting copy-move forged images (CMFD) poses a considerable challenge, especially when the alterations are subtle. In CMF, a portion of an image is intentionally copied and pasted within the same image, compromising its authenticity. Researchers employ diverse algorithms for forged image detection, focusing on feature extraction to identify tampered regions within images.

The manipulation of original images in web and social media, as illustrated in Figure 1, involves a range of photometric, geometric transformations, and copy-move forgeries facilitated by freely available image editing software like Adobe Photoshop Express, GIMP, PixlrE, PixlrX, Fotor, among others. Forging images through these tools results in distinct copies of the same image, leading to the need for forged image detection. Even when images are not exact replicas, they can still be visually recognized as the same picture, having undergone various editing stages such as color mapping, resizing, and format switching. This complexity underscores the importance of robust detection methods to identify and authenticate original images in the face of such manipulations.

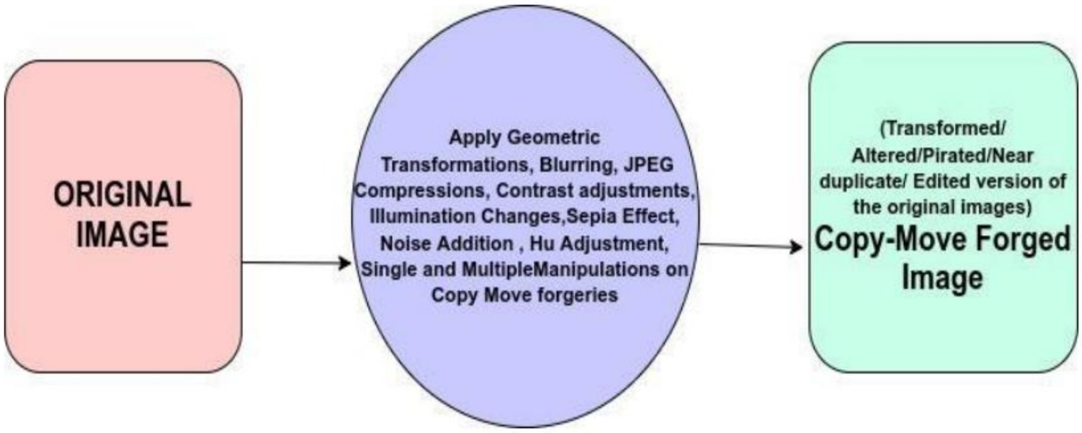
ORIGINAL IMAGE
Apply Geometric Transformations, Blurring, JPEG Compressions, Contrast adjustments, Illumination Changes,Sepia Effect, Noise Addition , Hu Adjustment, Single and MultipleManipulations on Copy Move forgeries
(Transformed/ Altered/Pirated/Near duplicate/ Edited version of the original images)
Copy-Move Forged Image

Fig 1 Manipulation/Creation of Forged Image

Copy-move image forgery (CMIF) stands out as a sophisticated image tampering technique, operating on the principle where an attacker strategically selects one or more regions (supply areas) and duplicates them by pasting into other parts of the same image (target areas) [4, 5]. This method allows for the creation of duplicate sections within the image, contributing to deceptive manipulations. To enhance the authenticity of the duplicated regions, attackers may employ additional strategies like adjusting brightness, contrast, size, and rotation. These alterations are aimed at making the replicated sections appear more natural and realistic, adding complexity to the detection of such forgeries.

Recognizing photo forgeries has become exceptionally challenging due to the striking resemblance of altered images to the originals. Advanced image editing software enables various modifications, falling into two categories: content modification and content protection [6]. The former type arbitrarily alters the semantic content and meaning of the image [7]. Such changes in content can convey incorrect or misleading information, emphasizing the importance of identifying manipulated images, especially as their prevalence grows. In recent years, detecting alterations in content, both in images and videos, has gained significance in surveillance applications. The copy-move image forgery illustrated in Figure 2 exemplifies the challenges posed by these manipulations.

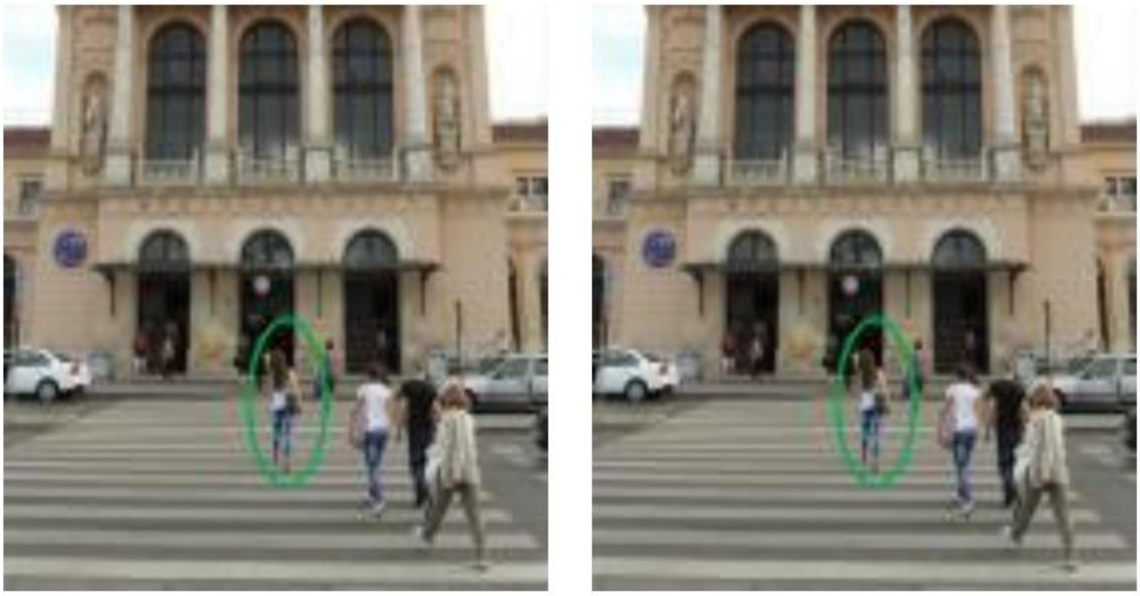

Fig 2: (a)authentic image(b) duplicate image

Textured components with random patterns, such as cloth, soil, grass, and trees, prove to be ideal for copy-move forgery, as the cloned components seamlessly blend into their surroundings, making it challenging to identify suspicious objects. The consistent dynamic range, color palette, noise variables, and other significant characteristics between copied and original portions, being from the same image, render them virtually undetectable by methods relying on statistical differences. Additional tools like Retouch or Feather Crop further obscure any traces of duplicated or shifted blocks, increasing the difficulty of fraud detection. Each instance of copy-and-paste fraud establishes a link between copied and original image blocks, forming a basis for recognition. Notably, the recognition algorithm must provide close matching between short image segments, operate efficiently with minimal false positives, and discern continuous segments in the forged image. In today's digital landscape, where information is predominantly conveyed through images, the need for authenticating digital photos and detecting forgeries becomes increasingly crucial. With easily accessible image processing and editing software, the significance of research in this domain is underscored. Furthermore, the following qualities highlight the significance of the research:

- This study introduces IKFR-T (Identical Key feature Recognition and Tracing), an automated system designed to address the challenge of copy-move forgery detection. IKFR-T optimally navigates three critical stages: counterfeit placement, similarity verification, and feature extraction (FE).
- In the initial FE step, image scaling and contrast optimization are applied for extracting SIFT key features from small and smooth areas. The second phase addresses key feature matching through an equality check. The model's resilience is enhanced in the final step through iterative localization rounds.
- The model's performance is assessed using three distinct standard datasets comprising altered and authentic images. Evaluation metrics at both image and pixel levels contribute to gauging the model's robustness.

- Comparative analysis with other models highlights IKFR-T's superiority in certain metrics, emphasizing its effectiveness in copy-move forgery detection.

2 Literature survey

Research has been conducted on several existing systems with a focus on the process of copy-move forgery detection, examining unintended consequences such as feature correlation among duplicated frames and the original frame. These consequences may manifest through frame replacement or frame insertion. This section provides a comprehensive review of various existing methods in video-based Copy-Move Forgery Detection (video-CMFD). The analysis delves into the intricacies of how these systems handle feature correlation and the challenges posed by frame manipulation in the context of video forgery. This review aims to offer insights into the strengths, limitations, and distinctive features of diverse approaches applied to video-CMFD.

The authors contribute a pioneering effort to address the semantic gap problem in copy-move forged detection, incorporating spatial pooling of local moment invariants for midlevel image representation. Their detection methodology extends traditional approaches in two significant ways: firstly, by introducing the bag-of-visual-words model into this domain, opening up a novel perspective for forensic study; secondly, proposing a word-to-phrase feature description and matching pipeline that encompasses the spatial structure and visual saliency information of digital images [6].

The authors present an innovative two-stage framework tailored for copy-move forged detection. The initial stage features a backbone self-deep matching network, incorporating atrous convolution and skip matching to enhance spatial information and leverage hierarchical features. Spatial attention is bolstered through self-correlation, strengthening the ability to identify regions with similar appearances. The second stage, termed Proposal SuperGlue, is introduced to eliminate false-alarmed regions and rectify incomplete regions [7].

The researcher introduces a novel approach for detecting copy-move forgery in digital images, employing the self-supervised image keypoint detector, SuperPoint. This approach harnesses the advanced capabilities of SuperPoint, integrating keypoint detection and descriptor extraction to accurately identify and localize copy-move forgery. A notable strength of this approach lies in its capacity to handle images with diverse textures, encompassing smooth and self-similar structural images [8].

A novel U-Net-like architecture, UCM-Net, is introduced, featuring multiple asymmetric cross-layer connections, self-correlation, and atrous spatial pyramid pooling (ASPP) between the feature extraction module (FEM) and tampered region localization module (TRLM) [9].

Additionally, a reptile search algorithm is proposed in conjunction with a deep transfer learning-based CM forged detection (RSADTL-CMFD) approach. This model utilizes the Neural Architectural Search Network (NASNet) for feature extraction, enabling effective capture of relevant and discriminative features from input images. To further enhance NASNet's performance, the reptile search algorithm (RSA) is employed for hyperparameter tuning [10].

The research endeavors to introduce copy-move forged detection algorithms employing advanced feature descriptors, including local ternary pattern, local phase quantization, local Gabor binary pattern histogram sequence, Weber local descriptor, and local monotonic pattern, coupled with optimized support vector machine and optimized NBC classifiers. These algorithms demonstrate efficient image classification, accurately distinguishing between copy-move forged and authenticated images, even in the presence of various attacks such as JPEG compression, scaling, rotation, and brightness variation [11].

3 Proposed Methodology

IKFR-T (Identical Key feature Recognition and Tracing) relies on feature extraction, similarity testing, and recursive localization. Figure 3 illustrates the IKFR-T workflow process. It is comprised of three stages: recursive localization, picture level optimization-optimized feature extraction, and similarity verification. Every stage has been refined, as has the mathematical expression for it.

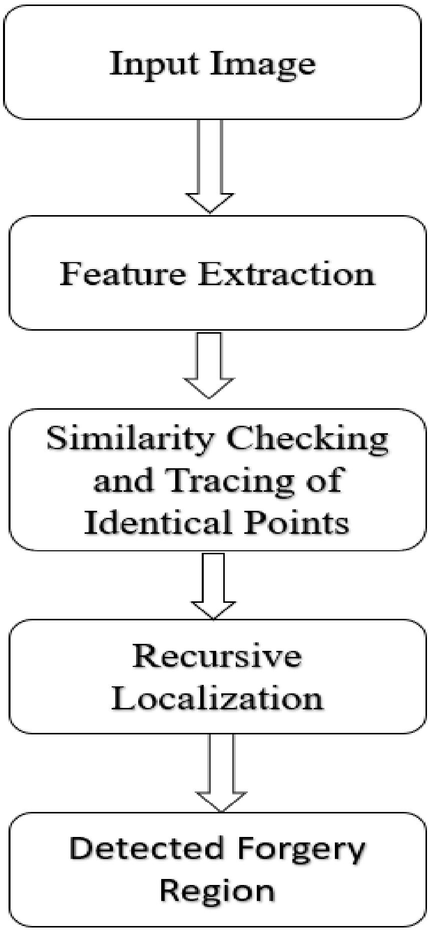

Fig 3 Architecture

3.1 Research Prelims along with FE (Feature Extraction)

SIFT is the most effective and simple way to extract key feature features; it is also the best approach for geometric alteration and noise distortion. In this section, we explore the use of the SIFT approach for key feature extraction and matching. The SIFT technique consists of the following four steps:

- Scale distance extremes recognition for the identification of key feature features.
- Key feature filtering using a specified contrast threshold and a specific edge

- Positioning each key feature in a tactical location.
- Acquiring the key feature description.

The next stage is to use a variety of scales to determine which aspects are most important.

The output picture Q, a Gaussian-distorted image, is produced by iteratively applying Gaussian-refinement at various scales to the input image. A parameter ψ domain cube with an axial length of three is then found to have its shared extrema containing the critical properties. The scaled-down form of DoG at φ is particularly emphasised as

$$\psi(y,z,\varphi) = M(y,z,y\varphi) - M(y,z,\varphi) \tag{1}$$

Here, $N(z,a,\varphi)$, represents the blurred Gaussian picture, and z is a previously established constant.

$$M(y,z,\varphi) = \zeta(y,z,\varphi) \otimes J(y,z) \tag{2}$$

In this case, the Gaussian kernel symbol is $\zeta(z,a,\varphi)$. The next step is to use edge and contrast criteria to exclude all important features. Because it rids the SIFT approach of its unnecessary extrema, this procedure is crucial. To produce rotational shifts, the final step is to place each important element at a critical location. Each point's (z,za,φ) position is calculated in the manner shown below:

$$\Theta(z,a,\varphi) = tan^{-1}\left((f_z)\ (f_y)^{-1}\right) \tag{3}$$

Here, the symbols f_z and f_y stand for the (z,a,φ)The gradient position data of the points included inside a common window at the SIFT's main feature is then used to construct a histogram of the locations. The primary location is the area with the greatest histogram value. The last phase evaluates a 128-dimensional descriptor by encoding the nearest information in a small region with a 16 by 16 scale space size that is located at the main feature of the SIFT. For the given picture H, a collection that includes the key features $\left\{key_{features1}, key_{features2}, \dots, key_{features0}\right\}$ and their matching descriptors $\{SF_1, SF_2, \dots, SF_{total}\}$ are created using the aforementioned four steps. Key, as specified by the vector key characteristics of the SIFT, is the mutual key feature. $key_{features} = \left(\left\{z_{key_{features}}, a_{key_{features}}, \varphi_{kkey_{features}}, \Theta_{key_{features}}\right\}\right)$ are the image plane positions; the primary position is denoted by $\Theta_{key_{points}}$, and the image plane positions are $\left(Zkey_{features}, za_{key_{features}}\right)$.

3.1.1 Feature Matching Technique

Usually, calculating the displacements between remaining $(o-1)$ key features concerning provided particular threshold did not perform well in given huge feature space in order to get the ideal key feature traces of $key_{features}$. Moreover, the nearest distance between is calculated throughout this operation. The distances assessed in the large feature space are mostly to blame for this. In particular, observe the Euclidean distance between the key feature key and the left over key feature $(O-1)$ in the specified ascending way for vector $f = \{f_1, f_2, \dots, f_O\}$. For example, $. f_1 \leq f_2 \leq \cdots \leq f_{O-1}$. If $(total-1)$ if $n > f_1/f_2$., the key feature key is then traced. In this case, , $n \in (0,1)$ is allocated already. In order to offer a better trace of the key feature, it is often not possible to calculate the displacements between the remaining $(o-1)$

$key_{features}$ with respect to a global threshold in large feature spaces. In this instance, the tracing approach is applied by determining the ratio of the closest distance to the following closest ones. It makes sense because there will likely be several erroneous routes close together given those problematic paths. This is a consequence of the huge feature space measurements being conducted so closely. Let us examine the growing Euclidean distance for the vector between the key feature key and the remaining key feature $(o-1).f =$ $\{f_1, f_2, \dots, f_O\}$ the distance of Euclidean among key feature key and left over key features $(O-1)$ in an ascending manner. i. e. $f_1 \leq f_2 \leq \cdots \leq f_{O-1}$. Therefore, if if $n > f_1/f_2$, then the key feature key is only related to any of the remaining $(total - 1)$ key features. In this case, $n \in (0,1)$. M is already allocated this time.

3.2 FE (Feature Extraction)

In this part of the study, we create a unique technique for detecting CM (Copy Move)-forgeries of an image by applying the SIFT approach for feature extraction. To evaluate the authenticity of a picture, three procedures are combined: Feature Point Extraction, Feature Point Tracing, and Repetitive Localization of Forged. Key characteristics properties are retrieved at this point. Since SIFT is the best technique for handling geometric transformation and noise distortion, we employ it to extract features. It is widely acknowledged that the primary issue with feature extraction based on key feature selection is that it is difficult to extract a sizable number of key features from small or delicate features, which exacerbates the situation. Additionally, we employ picture rescaling and contrast adjustment—two straightforward yet incredibly effective methods.

3.2.1 Image based enhancement

"Contrast threshold," or U, is the term used to describe the process of eliminating low contrast extremes that are deemed undesirable. For every distinct point in scale space with coordinates $x = (j, k, q)$, the contrast value is often shown as follows:

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

Here, $\widehat{w}$ represents $\widehat{w}$ location in linear space after filtering, and Eqn-1 acts as DoG,. Extrema with contrast levels less than U can't function as SIFT essential characteristics. On the other hand, it seems that soft areas have relatively low contrast values for the extrema. As a result, only few extrema—if any—can pass the contrast filtering test and turn into essential SIFT features. We use the U -reduction part of the SIFT method to ensure that, given the soft regions of the double, we can generate a sufficient number of important features. Since contrast optimisation alone is unable to provide exact essential characteristics, picture rescaling is an additional attempt to enhance the IKFR-T. As a result, image rescaling occurs prior to the computation of important characteristics. Additionally, resizing highlights a photo's strongest features.

3.3 Similarity checking

3.3.1 Tracing within image group:

In particular, the scale key ρ_{key} is thought to be aligned using the SIFT mechanism's key feature assessment. Additionally, b_p is the defined scale value in the qth octave. As you specifically analyse the SIFT key characteristics as key, take into account the relevance of any previously discovered ρ_{key} size. The scale of the first DoG picture is expressed as the q-th octave, denoted as α_p. The feature points are separated into three groups using our technique based on the scale values; these groups are denoted by the letters I_1, I_2, and I. True enough,

$$\begin{gathered} I_1 = \left\{key_{features_j} \middle| b_1 > \rho_{key_p} \geq b, k = 1, \dots, o\right\}, \tag{5} \\ I_2 = \left\{key_{features_j} \middle| b_2 > \rho_{key_p} \geq b, k = 1, \dots o\right\}, \tag{6} \\ I_3 = \left\{key_{features_j} \middle| \varphi_{key_{features_j}} \geq b_3, k = 1, \dots, o\right\}. \end{gathered}$$

The tracing process is then carried out on I_1, I_2, and I_3 separately. For the first and second octaves in particular, we use the tracing approach in each octave. But for the maximum number of octaves, we perform it integratively over multiple octaves. When categorising characteristics according to a scale, it is possible to identify the main traits within each group. We find that our strategy is far more successful than other currently used techniques.

3.3.2 Key features Partitions

The distance vector dist is assessed for the remaining major characteristics (I_1, I_2, and I_3) in the same group in order to provide important tracing possibilities. We want to make our tracing approach as efficient as possible because the number of key features acquired during feature extraction is high, and this efficiency often decreases as the number of key features rises. The formula for N is $N = \left\lceil \frac{255-d1}{e1-e2} \right\rceil + 1$ when every vector with a range of $[0, 1, \dots, 255]$that belongs to the M distinct classes has a step size of 1 and an overlay size of f_2, where f_1 is bigger than f_2. Additionally, let's examine a parameter d_p that has the following important characteristics, and where the $d_{p,i}$parameter has all of the F_q key features with grey values that are associated with the specified jth sub-level.

$$E_{q,j} = \left\{key_{features_k} | c\mu(key_{features_k}) < d, key_{features_k} \in E_q\right\}, \tag{7}$$

The grayscale values associated with important characteristics are defined by the μ parameter. An average is also computed; $\mathcal{P}_{p,i,}$ is then considered in a separate set with matching parameters of $c_{p,i}$and $\mathcal{P}$ is formulated.By calculating the average, the grey scale value corresponding to μ for the given key characteristics is found in the equation above. We also consider $\mathcal{P}_{p,i,}$ as a single set parameter consisting of matched pairs of $d_{p,i}$; moreover, $\mathcal{P}$ is calculated in this way.

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

3.4 Recursive localization method

3.4.1 Removal of the matched pairs

Furthermore, extra coordinated pairs are rejected by fulfilling the following equation for matched pairings $(key_{features}, \overrightarrow{key_{features}}) \in Q$; taking into account the dual parameter O_l and $\overrightarrow{O_l}$;; given distance as $key_{features}$ and $\overrightarrow{key_{features}}$ which is smaller than the specified threshold.

$$\max\{\overrightarrow{p_l}, p_l\} \geq p_\iota, \tag{9}$$

In the preceding equation, p_ι is taken to be equal to two. We further add the set parameter N, which is composed of the remaining matched pairs and is expressed as follows in notation:

$$O = \{(key_{features}, \overrightarrow{key_{features}}) | \max\{\overrightarrow{q_l}, q_l\} q_\iota; \; (key_{features}, \overrightarrow{key_{features}}) \in Q\} \tag{10}$$

3.4.2 Parameter evaluation

The above-mentioned estimate approach uses an affine matrix and only uses a small number of matched pairings from the predefined two areas. After selecting the matched pair, the matched key features that are closest to the $key_{features}$ and $\overrightarrow{key_{features}}$ are determined by taking into account the parameters 〚 $E_{key_{features}}$ and $E_{\overrightarrow{key_{features}}}$, with $\mathcal{M}_{keys}$ containing the matched key features in N and provided as:

$$\begin{aligned} E_{key_{features}} &= \{r | \forall r \in O_{keys}, \eta(q,l) < U_d\}, \\ E_{\overrightarrow{key_{features}}} &= \{r | \forall r \in O_{keys}, \eta(q,l') < U_d\} \end{aligned} \tag{11}$$

$$O_{keys} = \left\{ key_{features} \middle| \, \exists \overrightarrow{key_{features}}, s.t \, (key_{features}, \overrightarrow{key_{features}}) \in O \right\} \tag{12}$$

$$N_l = \{ < key_{features}, key_{features} > | \, key_{features} \in E_l \wedge \overrightarrow{key_{features}} \in E_{l'}; (key_{features}, \overrightarrow{key_{features}}) \in O\}. \tag{13}$$

3.4.3 Choosing parameter utilizing the image rotation

In order to illustrate the application of a dominant orientation strategy to improve estimation, we take into consideration a parameter Θ_l for a key feature that may be obtained by the SIFT method. Furthermore, J_l, the parameter is expressed as follows:

$$J_l = \begin{bmatrix} C & w \\ 0^T & 1 \end{bmatrix}, \tag{14}$$

The matrix $w = \left[w_y, w\right]^U$ in the preceding equation may be broken down using the transition vector t, the left singular vector u, and the right singular vector t. Together with the transition vector t, these vectors are employed.

$$\begin{aligned} \mathrm{C} &= \mathbb{ABC}^U = (\mathbb{AC})^u\ (\mathbb{CBC}^t) \\ &= \mathrm{T}\ (\Theta_I)\ T(-\Lambda_I)\mathbb{B}S(\Lambda_I), \end{aligned} \tag{15}$$

Furthermore, the unique parameter Θ_I may be used to obtain the rotational parameter and the B indicating factor's parameter can be obtained using the formula $\mathbb{B} = diag(\omega_1, \omega_2)$,.

$$T\ (\Theta_I) = \begin{bmatrix} cos(\Theta_I) & -\sin(\Theta_I) \\ \sin(\Theta_I) & \cos(\Theta_I) \end{bmatrix} = (\mathbb{BC}\ )^v. \tag{16}$$

Furthermore, copy-move patches can be turned in a clockwise or anticlockwise direction. In addition, to ensure uniformity, the value of Θ_I is determined by applying the following equation, which maps the value between the given range of 0 to 2π.

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

$$h(key_{features}, \overrightarrow{key_{features}}, I_l) = |\theta_{k'} - \Theta_I - \Theta_I\ |. \tag{18}$$

The estimated I_l, $h(key_{features}, \overrightarrow{key_{features}}, J_l)$, and the matched pair must all equal zero in order to achieve this aim. The requirements $h(key_{features}, key_{features}, I_l)\ \leq V_\Theta,\ \forall < V, \overrightarrow{key_{points}} > \in\ O_l$ must be met, with V_Θ standing for the pre-defined parameter. This condition has to be met if N_l is the inlier set that the recommended approach created. The dominant orientation parameter can be used to choose the inliers with matched pairs once an accurate calculation of J_l has been established. For the previously mentioned matched pair, the following equations may be written using the notation $\begin{pmatrix} \overrightarrow{y\ l} \\ \overrightarrow{z_l} \\ 1 \end{pmatrix} \approx I_l \begin{pmatrix} y_l \\ z_l \\ 1 \end{pmatrix}$. Additionally, the following equation may be used to compute M_H if the four crucial points $(y_l, z_l, \sigma_l, \Theta_I)$,—are taken into account:

$$O_K = \left\{ \begin{matrix} < key_{features}, \overrightarrow{key_{features}} > \\ g\left(key_{features}, \overrightarrow{key_{features}}, J_l\right) \leq U_{\Theta}; \left(key_{features}, \overrightarrow{key_{features}}\right) \in O \end{matrix} \right\}, \Bigg| \, \|Jl - \vec{l}\|_2^2 <\in O \qquad (19)$$

$$j_l = \arg min \sum_{<kkey_{features}, key_{features}> \in N_K} || \, Jl - \vec{l} \, ||_2^2 \qquad (20)$$

3.4.4 Optimal Forged localization

The first stage involves building the local suspicious region in the supplied N_k where the radius has the key point mentioned below; σ_k denotes the l scale value and the α hyperparameter.

The suggested model first tends to build the local forged region in O, where the radius and key point are provided by the following equations, with σ_k is standing for the l scale value and hyperparameter b. The model's first tendency is to create a local suspicious area in O_K.

$$t_l = \varrho \varphi_l. \qquad (21)$$

Next Step: At this level, region detection is approximated by examining and modifying the colour information; further transformation for each point is provided as follows:

$$key_{features\,*} = \hat{I}_l key_{features}, key_{features} \in U. \qquad (3.22)$$

$$R = \left\{ key_{features}, key_{features\,*} \middle| \max \left(\begin{matrix} |R(key_{features}) - \overline{R(key_{features})|}, |G(key_{features}) - \overline{G(key} \\ \left| G(key_{features}) - \overline{G(key_{features})} \right| \end{matrix} \right. < U_{rgb;} \, l \in T \right\} \qquad (23)$$

The formulas below are used to compute $\overline{R(key_{features})}$ where patch is defined as $\Omega(key_{features})$ and normalised using Z. Moreover, the formulas for $\overline{B(key_{features})}$ and $\overline{G(key_{features})}$ are also developed.

$$\overline{R(key_{features})} = \frac{1}{\mathbb{A}} \sum\nolimits_{key_{features} \in \Omega(key_{features})} R(key_{features}), \qquad (24)$$

Furthermore, we consider a parameter denoted as U', which has the following formulation:

$$key_{features} = \widehat{K}_l^{-1}\overrightarrow{key_{features}}, \overrightarrow{key_{features}} \in U'. \qquad (25)$$

Also, seeing T', we calculate R_2

$$R_2 = \{\overrightarrow{key_{features}}, \overrightarrow{key_{features}} *\left| \max\left(\begin{matrix} |R(\overrightarrow{key_{features}}) - \overline{R(key_{features} *)|}, |G(\overrightarrow{key_{features}}) - \overline{(G(\overrightarrow{key_{features}}))}|, \\ \left|G(\overrightarrow{key_{features}}) - \overline{G(\overrightarrow{key_{features}} *)}\right| \end{matrix} \right) \right. < V_{rgb;} \overrightarrow{key_{features}} \in U'\} \qquad (26)$$

Additionally, parameter D (binary mapping) is taken into account according on the input picture size; unit is used for forgery, and 0 is used for a specific spot. After that, parameter B is changed by taking into account points like S_1 and RS_2.

Lastly, one final parameter is assumed to have the same dimensions as the picture supplied into the system; this value is D and is utilised for the binary map. This assumption was formed because, at this point, the forged sections are indicated by the notation unit, while the true position is shown by the notation zero. Furthermore, it is claimed that the value of parameter C is modified by considering points S and S_2,.

$$\mathbf{D}(S_1 \cup S_2) = 1. \qquad (27)$$

Furthermore, the suggested model is able to generate the forged areas by the sequential approach once the iteration process is finished. When the model has gone through every iteration, this will be feasible. Given that the model solves issues in a sequential manner, this is a possibility. In order to do this, the minuscule bits are disposed of and the remaining open sections undergo the close process. Furthermore, a photograph is deemed genuine only if its worth is zero; if it has any other value, it is deemed fraudulent. An picture is regarded to be fabricated if its value is not zero.

4 Results and Discussion

In this section, we showcase the outcomes and conduct a thorough examination of the results within the context of copy-move forgery detection. The effectiveness of the proposed methodology is evaluated through a meticulous assessment, taking into account key performance metrics. The subsequent discussion explores the strengths, limitations, and notable observations, illuminating the algorithm's robustness and areas with potential for improvement. By undertaking a comparative analysis involving existing models and GRIP datasets [16], our objective is to offer valuable insights into the progress and challenges in the domain of copy-move forgery detection.

4.1 Dataset description

The GRIP dataset comprises both global and regional vector datasets available in ESRI file geodatabase and shapefile formats, along with global raster datasets illustrating road density. The dynamic regions within the 160 photos of the GRIP dataset exhibit arbitrary shapes and sizes, ranging from 400 to 5,000 pixels.

4.2 Metrics comparison

IKFR-T undergoes evaluation at both pixel and image levels, focusing on its ability to distinguish between authentic and manipulated images. This study assesses the model's dependability and efficiency in identifying altered regions at the pixel level. Performance metrics consider the original and modified images or pixels as positive and negative samples, respectively. Key metrics such as F1-Score, True Positive Rate (TPR), and False Positive Rate (FPR) are employed for a comprehensive evaluation. TPR signifies the identification of genuinely manipulated images within the detection zone and is computed as TPR = Recall / (True Positive Rate) / (False Positive Rate).

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

Similarly, the False Positive Rate (FPR), which ideally should be minimized, represents the total count of photos erroneously classified as tampered images.

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

The count of manipulated pixels or images correctly identified as genuine is termed false negative, while the count of manipulated pixels or images incorrectly identified as forged is known as true negative. F1, representing the harmonic mean of recall rate and accuracy, serves as a comprehensive evaluation metric, with increased likelihood of reflecting experimental data accuracy as F1 approaches its maximum value. While F1-pixel operates at the pixel level, TPR, FPR, and F1-picture are implemented at the image level.

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

4.3 GRIP dataset

4.3.1 Image based analysis

The hierarchical approach achieves a 100% F1-score; however, all other methods, except for Hierarchical, exhibit FPR values above 0.0, with IKFR-T recording an FPR value of 0.036145. With an impressive TPR score of 100% for all models except one, the mentioned models perform exceptionally well. Refer to Table 1 and Figure 4 for a detailed comparison at the image level.

Table 1 Comparisons at Image level

Methodologies	F1-Score	FPR	TPR
Heirarchical [13]	100	0	100
Iterative [14]	85.56	33.75	100
PM-ZM [15]	97.53	6.25	98.75
ES [12]	91.72	10.42	90
PS	98.08	0.036145	100

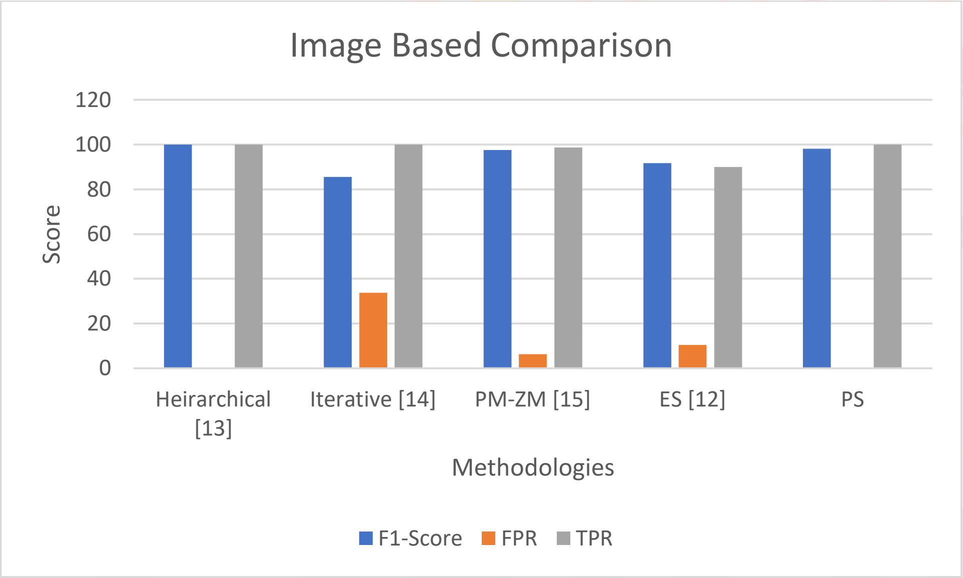

Fig 4 Image Level Comparison

4.3.2 Pixel based analysis

The proposed model attains a 99.72% accuracy, matching the previous model's accuracy, while outperforming the other model with a higher F1-score. Table 2 and Figure 5 provide a comparison of various strategies at the pixel level, focusing on F1 score, precision, and recall metrics. In terms of precision, the suggested model achieves 100%, surpassing the present model's 99.96%; previous models did not calculate precision. Furthermore, IKFR-T achieves a recall value of 99.02, outperforming the previous model's recall rating of 98.59.

Table 2 comparisons (Pixel level)

Methodologies	F1-Score	Precision	Recall
Heirarchical [13]	94.66	NA	NA
Iterative [14]	66.44	NA	NA
PM-ZM [15]	96.15	NA	NA
ES [12]	99.72	99.96	98.59
PS	99.46	100	99.02

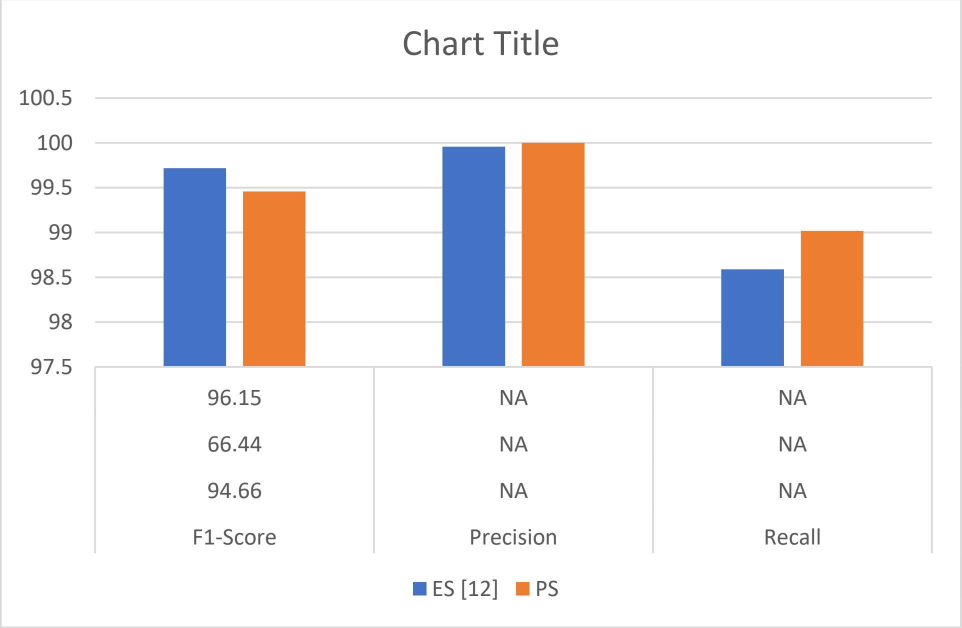

Fig 5 Pixel based analysis

4.4 Comparative analysis

The proposed IKFR-T (Identical Key Feature Recognition and Tracing) methodology, centered around Identical Key Feature Recognition and Tracing, surpasses existing models in copy-move forgery detection. With a pixel-level accuracy of 99.72%, it demonstrates superior performance compared to other methods, accompanied by a minimal False Positive Rate (FPR) of 0.036145 at the image level. Despite achieving a 100% F1-score, the hierarchical approach falls short in terms of FPR. Meticulous key feature extraction, similarity checking, and recursive localization contribute to the methodology's robustness and efficacy. This research signifies a noteworthy advancement in the field, highlighting the potential of the proposed methodology for image analysis.

5 Conclusion

The proposed IKFR-T (Identical Key Feature Recognition and Tracing) methodology demonstrates remarkable effectiveness in copy-move forgery detection, outperforming existing models in precision, recall, and overall accuracy. By leveraging the SIFT method and recursive localization, IKFR-T addresses key challenges in feature extraction, similarity checking, and localization, ensuring robust performance in diverse scenarios. The utilization of the GRIP dataset further validates the methodology's real-world applicability. The research underscores the significance of incorporating image rotation, dominant orientation, and sequential processing for optimal forged localization. IKFR-T represents a promising advancement in the field, providing a comprehensive solution to the intricate problem of copy-move forgery in digital images. Future work may explore further optimizations and extensions of the proposed methodology to enhance its versatility and applicability in evolving digital landscapes.

6 Acknowledgements

We express our profound appreciation to everyone who has supported and contributed to this research endeavor. Specifically, we extend our heartfelt gratitude to our mentor for providing unwavering guidance, invaluable insights, and continual encouragement throughout the entirety of this research journey. It's important to note that no funding granted for this research.

References

1. K. M. Hosny, A. M. Mortda, M. M. Fouda and N. A. Lashin, "An Efficient CNN Model to Detect Copy-Move Image Forged," in *IEEE Access*, vol. 10, pp. 48622-48632, 2022, doi: 10.1109/ACCESS.2022.3172273.
2. N. T. Pham and C. -S. Park, "Toward Deep-Learning-Based Methods in Image Forged Detection: A Survey," in *IEEE Access*, vol. 11, pp. 11224-11237, 2023, doi: 10.1109/ACCESS.2023.3241837.
3. A. H. Khalil, A. Z. Ghalwash, H. A. -G. Elsayed, G. I. Salama and H. A. Ghalwash, "Enhancing Digital Image Forged Detection Using Transfer Learning," in *IEEE Access*, vol. 11, pp. 91583-91594, 2023, doi: 10.1109/ACCESS.2023.3307357.
4. S. Teerakanok and T. Uehara, "Copy-Move Forged Detection: A State-of-the-Art Technical Review and Analysis," in IEEE Access, vol. 7, pp. 40550-40568, 2019, doi: 10.1109/ACCESS.2019.2907316.
5. K. H. Rhee, "Generation of Novelty Ground Truth Image Using Image Classification and Semantic Segmentation for Copy-Move Forged Detection," in IEEE Access, vol. 10, pp. 2783-2796, 2022, doi: 10.1109/ACCESS.2021.3136781.
6. C. Wang, Z. Huang, S. Qi, Y. Yu, G. Shen and Y. Zhang, "Shrinking the Semantic Gap: Spatial Pooling of Local Moment Invariants for Copy-Move Forged Detection," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1064-1079, 2023, doi: 10.1109/TIFS.2023.3234861.
7. Y. Liu, C. Xia, X. Zhu and S. Xu, "Two-Stage Copy-Move Forged Detection With Self Deep Matching and Proposal SuperGlue," in IEEE Transactions on Image Processing, vol. 31, pp. 541-555, 2022, doi: 10.1109/TIP.2021.3132828.
8. A. Diwan, D. Kumar, R. Mahadeva, H. C. S. Perera and J. Alawatugoda, "Unveiling Copy-Move Forgeries: Enhancing Detection With SuperPoint Keypoint Architecture," in *IEEE Access*, vol. 11, pp. 86132-86148, 2023, doi: 10.1109/ACCESS.2023.3304728.
9. S. Weng, T. Zhu, T. Zhang and C. Zhang, "UCM-Net: A U-Net-Like Tampered-Region-Related Framework for Copy-Move Forged Detection," in *IEEE Transactions on Multimedia*, vol. 26, pp. 750-763, 2024, doi: 10.1109/TMM.2023.3270629.
10. M. Maashi *et al.*, "Modeling of Reptile Search Algorithm With Deep Learning Approach for Copy Move Image Forged Detection," in *IEEE Access*, vol. 11, pp. 87297-87304, 2023, doi: 10.1109/ACCESS.2023.3304237.
11. S. B. G. T. Babu and C. S. Rao, "Copy-Move Forged Verification in Images Using Local Feature Extractors and Optimized Classifiers," in *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 347-360, September 2023, doi: 10.26599/BDMA.2022.9020029.

12. B. Chen , W. Tan , G. Coatrieux , Y. Zheng , Y. Shi , A serial image copy-move forged localization scheme with source/target distinguishment, IEEE Trans. Multimedia (2020) .
13. D. Cozzolino, G. Poggi, and L. Verdoliva, ‘‘Efficient dense-field Copy– Move forged detection,’’ IEEE Trans. Inf. Forensics Secur., vol. 10, no. 11, pp. 2284–2297, Nov. 2015.
14. Y. Li and J. Zhou, ‘‘Fast and effective image copy-move forged detection via hierarchical feature point matching,’’ IEEE Trans. Inf. Forensics Security, vol. 14, no. 5, pp. 1307–1322, May 201.
15. M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour, ‘‘Iterative copymove forged detection based on a new interest point detector,’’ IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2499–2512, Nov. 2016,
16. H. Chen, X. Yang and Y. Lyu, "Copy-Move Forged Detection Based on Keypoint Clustering and Similar Neighborhood Search Algorithm," in *IEEE Access*, vol. 8, pp. 36863-36875, 2020, doi: 10.1109/ACCESS.2020.2974804.