International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Detection of Copy-Move Forgery (CMF) in Videos through the Application of a Machine Learning Algorithm

[1]Sampangirama Reddy B R, [2]Mohan Vishal Gupta, [3]Pawan Bhambu, [4]Alka Singh

Submitted:17/04/2023 **Revised:**06/06/2023 **Accepted:**22/06/2023

Abstract*:* One of the most important tasks in digital forensics to find instances of modified content is the detection of copy-move forgery (CMF) in videos. Copy-move forgery includes taking a section of a video, pasting it into another movie, and then hiding or changing that section. As a consequence of advancements in network technology, low-cost multimedia devices, intelligent image or video editing software, and broad adoption of digital multimedia coding standards, the number of applications for digital multimedia has significantly risen in recent years. Establishing if a video is legitimate or not is one of the trickiest areas of video forensics. This may be a crucial responsibility when recordings are used as primary evidence to influence decisions, such as in a court of law. Therefore, we provide a novel machine learning-based copy-move forgery detection technique in this research. Weiner filter is first used to gather and pre-process video data. The pre-processed video data are then segmented using a threshold-based technique to image segmentation. Finally, we suggest a novel integrated stochastic random neighbouring approach (ISRNA) for categorizing videos. Our suggested technique is compared and contrasted with traditional ways to demonstrate the efficacy of the suggested method. Results from experiments show that our suggested strategy performs better than traditional ways.

Keywords: *Copy-Move forgery (CMF), weiner filter (WF), threshold based image segmentation (TbIS), integrated stochastic random neighbouring approach (ISRNA)*

1. Introduction

A specific kind of image tampering called CMF involves copying a portion of the image and placing it someplace else in the image to hide a significant visual characteristic. Consequently, the objective of Copy-Move Forgery Detection (CMFD) is to detect image fields that are identical or highly comparable. A CMF, a section of the original image is copied, then pasted in another location on the same image to conceal important objects or add more information that was not originally included in the image [1]. The statistical method involves breaking the image up into patches and using two different ways to match the patches together. One is a strong match, while the other is an exact match. However, when no action is carried out across the duplicated area, this strategy performs well. The process of video forgeries involves altering or eliminating certain things from the video sequence. Splicing and copy-move are two kinds of extant forging methods. The gaps among the video frames are used in intra-frame forgery detection to find any forgeries. These techniques include splicing and CMF. This method is used to change the image frames in videos [2]. Splicing is a kind of image manipulation that includes replacing a predetermined number of image blocks or parts from the test-target digital image with new ones. A standard approach is used to look for discrepancies between the test and target images' characteristics, values, or attributes. Although it is important to have appropriate algorithms for both of these associated paradigms [3]. Digital visual forgery is the fabrication of images using altered original data from images. One of the many image-manipulation techniques that may be used to create a fake image is copy motion counterfeiting. Cutting out a portion of a photo, duplicating it, and pasting it into another position or location within the same

photograph constitutes CMF [4]. The conversion of RGB to grayscale, HSV, YCbCr, local binary patterns, and principal component evaluation, are often used CMFD pre-processing methods that decrease the dimensionality of the image and hence speed up processing or improve detection accuracy. The ability of the whole detection relies on the features collected, making this the most important phase in CMFD. The image's interesting details are captured. Matching involves comparing recognized traits to find commonalities [5]. One of the most effective methods for

1Assistant Professor, Department of Computer Science and IT, School of Sciences, Jain (Deemed-to-be University), Bangalore-27, India, Email Id: sampangi.reddy@jainuniversity.ac.in

2Assistant Professor, College of Computing Science and Information Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India, Email id: mvgsrm@indiatimes.com

3Associate Professor, Department of Computer Science & Engineering, Vivekananda Global University, Jaipur, India, Email Id: pawan.bhambu@vgu.ac.in

4Assistant Professor & Department of Master of Computer Application, Noida Institute of Engineering and Technology, Greater Noida, Uttar Pradesh, India, Email id: alkasingh.it@niet.co.in

enabling people to currently obtain large amounts of information is still the digital image. It is stated that an image is worth a thousand words, which explains how much information an image has. The amount of digital images has considerably increased with the introduction of new cameras, smartphones, and tablets. Such propagation has been further aided by social media platforms like Facebook, Instagram, and Twitter. Additionally, software for digitally altering these photographs has been steadily improved, and programs like Photoshop, Gimp, and mobile apps like Snapseed and Pixlr make it relatively simple for users to transform images [6]. Another common approach used nowadays for image forgeries is the copy-move technique, in which one portion of an image is utilized to conceal another section from the same image. Two identical sections are unusual in natural photographs, therefore this attribute may be utilized to spot these kinds of alterations. There will be two quite identical portions in the altered image, even after using various post-processing techniques, such as edge smoothing, blurring, and adding noise to remove obvious signs of tampering [7]. The rapid development and use of image and video editing programs similar to Adobe Premiere, Photoshop, and Final Cut Pro make it simpler to manipulate digital visual material without leaving clear signs of tampering. Malicious tampering, however, might result in significant societal and legal issues. For instance, altered photos or videos might be used as fake testimony in court or to deceive the public about the veracity of news stories [8]. Hence, for efficient detection of copy-move forgery (CMF) in videos, we proposed integrated stochastic random neighbouring approach (ISRNA) modeling.

2. Related work

The research [9] employed several convolutional layer stages and multi-scale input to create a deep-learning CNN model. CMF, being a member of the worst forgery attacks, is a significant source of information in the form of images. Its goal is to keep private information out of the image. The article [10] produced altered images by hiding undesirable things or duplicating appealing objects in the same image. Digital images have become pervasive and are capable of being created and altered by a broad range of hardware and software technologies. CMF is a technique for altering images that involves concealing undesired elements or replicating appealing ones inside the same image. The study [11] determined to iterative localization technique uses the resilience characteristics of each key point and its color data to find the forged area. Employing scale clustering, overlapping grey scale clustering, and group matching modules, a unique multi-scale matching approach is created. The internet has been more widely used, production it easier to broadcast and buy digital information. The widespread use shows that the vulnerability of multimedia to alteration has risen as a result of counterfeiting. The article [12] continued a digital video forensics investigation into the consequences of hacking and video manipulation methods, and it emerged as a remedy for the issue of digital media's lack of credibility. One of the most frequent assaults is copy-move manipulation, which also includes versions for deleting and duplicating objects in films. The attack has been the subject of several video forensics studies using various methodologies. The research [13] provided a unique method for identifying frame copy-move forgeries while taking into account the three conditions. Based on optical flow (OF) and stable parameters, a coarse-to-fine detection approach is developed. To locate potentially manipulated locations, coarse detection evaluates OF sum consistency. The research [14] presented a brand-new technique for detecting copy-move forgeries is put forward. The widespread use of inexpensive image-altering software, fake photographs have developed into serious societal issues with very negative consequences. When copying and pasting portions of an image addicted to alternative area of the same image, the CMF method is often employed to manipulate images. The study [15] determined a collection of 250 original movies that have been altered mostly through the forging methods of insertion and deletion. One technique of alteration is covertly inserting transparent objects into the original footage. The collection also contains examples of forgeries where items from the original film have been removed without the viewers' knowledge. The work [16] described a technique for image authentication. The suggested technique uses the discrete cosine transform to identify copy-move modifications inside an image. We may create transfer vectors, which are clustered together, using the properties we learn from these coefficients. A tolerance threshold may be used to assess if any areas of the analysed image have been copied and pasted. The article [17] employed SIFT, invariant moments analysis, and the region expanding the technique to find the copy-move forgeries areas. The essential elements of an image are first gathered using SIFT-based key points. Then, all potential pair blocks of the copy-move areas are identified by looking at pairs of key points with closed scales. Third, the orientations are changed to be the same for each pair of matching key points. The paper [18] provided accessibility of image editing technologies have significantly reduced the costs, expenses, and skills required to profit from and sustain compelling visual tampering. Modified photographs are disseminated all over the globe with the help of reliable internet platforms like Facebook, Twitter, and Instagram. Operators of internet stages may be ignorant of the presence and dissemination of fake photographs. The research [19] described a passive blind method for detecting frame and region duplication fraud in movies. The method combines two separate methods. The

three different types of video frame duplication forgery copying a run of consecutive video frames at a long continue position, copying many of these runs of varying lengths at various locations, and copying from other videos with changed and identical dimensions can cause serious issues in real-world settings.

3. Methods

An essential challenge in digital forensics and multimedia analysis is the identification of Copy-Move Forgery (CMF) in videos. A certain area of an image is copied and pasted onto another position within the same image in a process known as CMF. Data from the video is initially gathered and pre-processed using the Weiner filter. A threshold-based approach to image segmentation is used to segment the pre-processed video data after that. We propose an innovative Integrated Stochastic Random Neighbouring Approach (ISRNA) technique for classifying films. The suggested block diagram is shown in Figure 1.

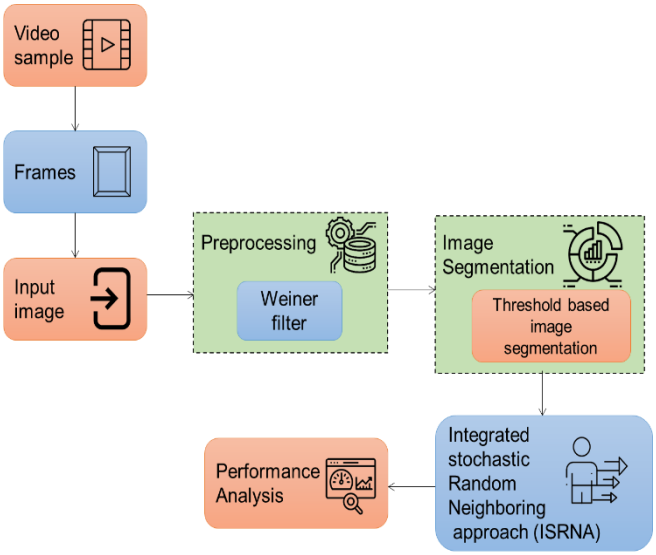

Fig.1. Block diagram of proposed

3.1. Data collection

There is a broad variation in the parameters, rotational angle, and scaling factor that have been employed. This collection only contains a very small number of images, which may not be sufficient to accurately assess a copy-move technique's performance. The size of the images, the absence of post-processing attacks, the significant variation in the dimension of the copy-move zone, and the inconsistent degrees of rotation and scaling attacks are only a few of the drawbacks this dataset (20). The dataset's contents are shown in Table 1 of the document.

Table 1. The dataset for the Copy-Move Hard (CMH) operation

Subset	Attack	Overview	Number of images
CMH_{P1}	Plain	A simple example where the duplicated region was simply shifted after copied.	29.8
CMH_{P2}	Rotation	Images with the replicated region rotated (angles between -90 degrees and 180 degrees)	24.6
CMH_{P3}	Scaling	Images having the copied area resized (scaling factors ranging from 80 percent to 154 percent)	25.9
CMH_{P4}	Combined	Images that combine scaling and rotation	33.7
Total			108

3.2. Pre-processing of the Wiener filter

Enhancing the quality of an image by eliminating pointless distortions Pre-processing's goal is to improve specific aspects so that the image can be examined properly. The pre-processing comprises brightness modification, image scaling, conversion, and filtering. The two stages used for pre-processing the input images, which are initially started, are noise elimination and image resizing.

$$E_n = E_1, E_2, E_3, \ldots E_N \quad (1)$$

Where E_n is the requested number of input images. The

Wiener Filter (WF) is then used to eliminate the noise during the noise mitigation procedure. The WF analogizes the received signal and the predicted noise-removal signals to reduce the noise. Both the noise-damaged frequency components and the parts of the traditional WF that can be restored by the filters cannot be recovered. To overcome the aforementioned problems, The Borel Transform (BT) is used in the WF instead of the Fourier transform. The mitigation noise image $E_{n(NR)}$ is described as

$$E_{n(NR)} = WF(E_n).RS(E_n) \quad (2)$$

Where the data that was received is identified as$RS(E_n)$. The input image was processed using the Wiener filter $WF(E_n)$ is interpreted as

$$WF(E_n) = \frac{BT"(E_n)}{|BT(E_n)|^2 + \frac{\Delta_S(E_n)}{\Delta_N(E_n)}} \quad (3)$$

where $BT(.)$ is used to denote the BT. The inverse of the point spread function The power spectrum of the signal process is denoted as Δ_s, while the power spectrum of the noise process is denoted as Δ_N. BT is represented as $BT(.)$. The BT is represented by,

$$BT(E_n) = \int_0^\infty T(u)e^{-E_n u}\, du \quad (4)$$

where T represents the complex function obtained by using the complex parameters. The noise-removed images $E_{n(NR)}$ are then downsized to 512×512, which is then supplied as,

$$E_{n(NR)} \underset{\rightarrow}{resizeto512 \times 512} E_{n(512\times512)} \quad (5)$$

Where the label for the enlarged image states$E_{n(512\times512)}$.

3.3. Segmentation of Threshold-based image segmentation

Threshold is a common method for dividing up images into distinct parts. It is a handy tool for setting the scene's background and forefront apart. By adjusting the amount of the threshold T, the grayscale image could be converted to a binary one. All relevant information on the whereabouts and appearance of the target objects needs to be encoded in the binary image. When starting with a binary image, recognition, and categorization are accelerated due to the reduced complexity of the data. The most common method for converting a grayscale image to a binary one is to use a single threshold value. Every grayscale value below this threshold will be labeled as zero (0), while those over will be labelled as one. Consequently, determining an appropriate threshold T value becomes the segmentation problem. One popular method for selecting T is to examine the various image types that need to be segmented. In the ideal scenario, the information presented would only display two significant flows and a clear flat. In this case, the value of T is selected as the boundary between the two modes. The histograms produced by real-world applications are more complex, with several peaks and murky valleys, making it difficult to determine an appropriate value for T.

$$g(x,y) = f(x) = \begin{cases} 1, if\ f(x,y) > T \\ 0, if\ f\ (x,y) \le T \end{cases} \quad (6)$$

An object point in an image is any point (x,y) where$f(x,y) > T$; alternatively, the area serves as a scenic background, the segmented image$g(x,y)$. When the intensity distributions of the foreground and background pixels in the images are sufficiently different, it is feasible to employ a single (global) threshold that applies to the whole image. Global thresholding is an acceptable choice, but in most applications, there is sufficient variance between images that an algorithm that can predict the threshold value for each image is required. The following are the key stages of the iterative process that the global threshold employs.

1. Choosing a starting point for the international threshold, T.
2. Segmenting the image using $g(x,y) = f(x) = \begin{cases} 1, if\ f(x,y) > T \\ 0, if\ f\ (x,y) \le T \end{cases}$ this will result in two sets of pixels: G1, which includes all pixels with intensity values$> T$, and G2, which includes all pixels with quantities$\le T$.
3. Calculating the pixels in G_1 and G_2's mean intensity values, m_1 and m_2,
4. Make a new threshold calculation: $T = \frac{1}{2}(m_1 + m_2)$Steps 2-4 should be repeated until the mean values remain the same after many repetitions.

This approach performs well when the histogram's modes corresponding to objects and background are separated by a relatively distinct valley.

3.4. Illumination

A dimensionality reduction technique called SN aims to duplicate the local structure of high-dimensional information in a low-dimensional environment. Since it is based on comparing distances across distributions, the SN technique is distinct from previous approaches since it employs a fundamentally smooth aim. SN creates an average $pi(j)$ for each point i that gives it's near neighbors an increased chance given a collection of high-dimensional indications $\{x_1, \ldots, x_n\}$:

$$p_i(j) \propto exp\left\{-\frac{\|x_i - x_j\|^2}{2\sigma_i^2}\right\} \quad (7)$$

The pattern of distribution is highly influenced by the length-scale σ_i^2 this is selected to reduce the amount of entropy of p_i to a particular amount supplied by the userσ_i^2. In this manner, the values of p_i explain the high dimensional information of local neighborhood structure in an evolving manner.

A collection of values is given$\{Z_1, \ldots, Z_n\}$ according to define a comparable probability in a low-dimensional space $q_i(j) \propto exp\left\{-\left\|z_i - z_j\right\|^2\right\}$ it explains how the embedded points are arranged in the closest distance.

By reducing the following aim, SN locates a strong local neighborhood structure that is similar to the initial information.

$$\sum_i KL(p_i||q_i) = -\sum_i \sum_j p_i(j) log q_i(j) + const. \quad (8)$$

While other approaches of dimensionality reduction, such as multidimensional scaling, reward configurations that spread out points, SN rewards those that bring distant points closer together.

Multiple enhancements have been made to SN. Uni-SN changes the meaning of q_i(j) by introducing a minor constant$q_i(j) \propto exp\left\{-\left\|z_i - z_j\right\|^2\right\} + k$. SN now has access to more "effective space" in the low-dimensional space while the system is presently able to position distant points in any direction. t-SN redefines in a different way of q_i(j) more dramatically, to$q_i(j) \propto \left(1 + \left\|z_i - z_j\right\|^2\right)^{-1}$, However, tends to function even better owing to the Cauchy distribution's thicker tails. A group of machine learning or regression trees, each built from a random resampling of the initial data used for training, make up the Random Forests technique. A training set is indicated by $\mathcal{L} = \{(x_i, y_i), i = 1,2, \ldots, N\}$ using N as the total number of samples, $x_i$is the matrix of characteristics $y_i \in \{1,2, \ldots, C\}$ is the nth sample used to teach a model. Tree learners and the idea of aggregating bootstraps or tree bagged before they go into the specifics of the Random Forest technique. Bagging takes a training set L and continuously conforms trees to subsets of that set, where L is replaced with a random number.

There are B iterations of this procedure. At each step$b$, N instances are randomly selected from L to formL_b, and the L_b is then used to train a regression treef_b. By summing the forecasts of all the various regression models onx_t, we may predict the result of unknown instances x_t after training.

$$\hat{f} = \frac{1}{B}\sum_{b=1}^{B} \hat{f}_b\,(X_t) \quad (9)$$

The bootstrapping method improves model performance by reducing variance without altering bias. Since B is a free parameter, we may determine its value using cross-validation or by measuring the out-of-bag error, or the average amount of incorrect predictions made by each training sample x_i when utilizing just the trees that do not involve x_i in their bootstrap sample. However, in practice, random forests employ an altered tree method of learning called feature bagging, which picks a random subset of the features for every potential split in the process of learning. It is common practice to use feature bagging to improve feature space exploration by decreasing tree-to-tree connection.

4. Performance Analysis

In this part, the suggested system's effectiveness is evaluated. The performance indicators used for evaluation are accuracy, precision, F-measure, specificity, and sensitivity. The existing techniques utilized for comparison are Binary Discriminative Feature (BDF), Speeded Up Robust Feature (SURF), and Oriented FAST and rotated BRIEF (OFB).

4.1. Accuracy

The fraction of accurately recognized image pixels is referred to as accuracy. A further name for this involves absolute image accuracy. While providing the most basic performance indicator, if there is a class conflict, it can outcome in inaccurate image detection results. A grouping discrepancy exists when one recognized group operates better than another. In this instance, biased outcomes would result from the dominating class's higher accuracy outweighing the inferior accuracy of the opposing group. For assessing detection outcomes using images, the accuracy measure was suggested if there was no group disagreement. Figure 2 demonstrates the comparable values for the accuracy measures. In Table 2, the accuracy of the suggested method is contrasted with the existing methods. In comparison to existing methods, the suggested approach offers a high level of accuracy. Accuracy is assessed using equation 10.

$$Accuracy = \frac{t_p + t_n}{t_p + t_n + f_p + f_n} \quad (10)$$

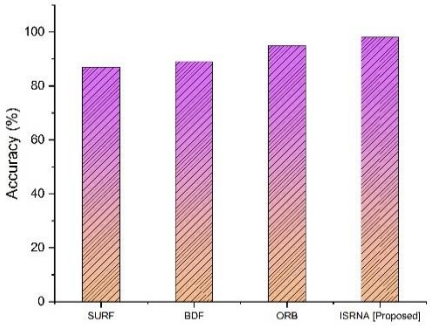

Fig.2. Accuracy comparisons between the suggested and current approaches

Table 2. Comparison of Accuracy

Method	Accuracy (%)
SURF	87
BDF	89
ORB	95
ISRNA [Proposed]	98

4.2. Precision

The most crucial standard for accuracy is precision, it is clearly defined as the percentage of properly categorized cases in all instances of predictively positive data. Equation (11) is used to compute the precision. A common method of manipulating digital images is called CMF, which involves copying a portion of the image and pasting it in a different location inside the same image in an attempt to deceive users or change the content. Figure 3 demonstrates the comparable values for the precision measures. In Table 3, the precision of the suggested method is contrasted with the existing methods. In comparison to existing methods, the suggested approach offers a high level of precision.

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (11)$$

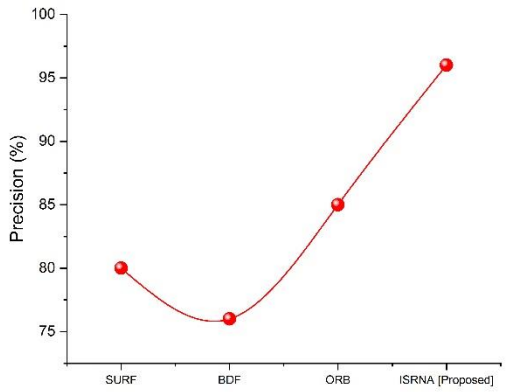

Fig.3. Precision comparisons between the suggested and current approaches

Table 3. Comparison of Precision

Method	Precision (%)
SURF	80
BDF	76
ORB	85
ISRNA [Proposed]	96

4.3. F-measure

The performance of the suggested and existing techniques is assessed using the F-measure. A higher F-measure result demonstrates its better ability to detect the CMF in digital images. Equation (12) describes the F-measure. Figure 4 demonstrates the comparable values for the F-measure. Table 4, the F-measure of the suggested method is contrasted with the existing methods. In comparison to existing methods, the suggested approach offers a high level of F-measure.

$$F - measure = 2 \times {}^{\text{Tp}}/_{2 \times (\text{Fp} + \text{Fn} + \text{Tp})} \quad (12)$$

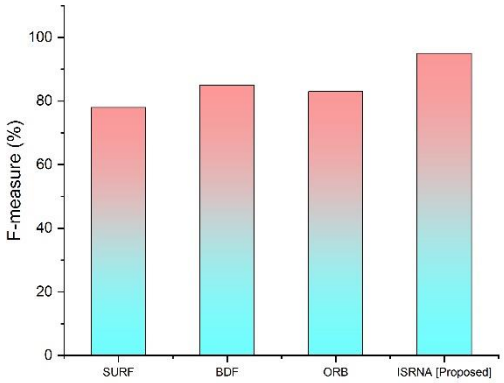

Fig.4. F-measure comparisons between the suggested and current approaches

Table 4. Comparison of F-measure

Method	F-measure (%)
SURF	78
BDF	85
ORB	83
ISRNA [Proposed]	95

4.4. Specificity

Specificity in the context of copy-move fraud detection relates to a detection method's ability to accurately recognize areas in an image that are real and untouched. Based on all the places the detection system flagged as non-manipulated, it calculates the percentage of real negatives. Specificity is an important parameter since it shows how effectively a copy-move fraud detection method can prevent false alarms or incorrectly mark valid portions of an image as modified. With a high specificity score, the approach is more likely to reliably detect unmodified areas and have a low number of false positives. A lesser number of false positives would be indicated by greater specificity. Figure 5 demonstrates the comparable

values for the Specificity measures. Table 5, shows the specificity of the suggested method is contrasted with the existing methods. In comparison to existing methods, the suggested approach offers a high level of Specificity. Equation (13) describes the Specificity.

$$Specificity = \frac{TN}{TN+FP} \quad (13)$$

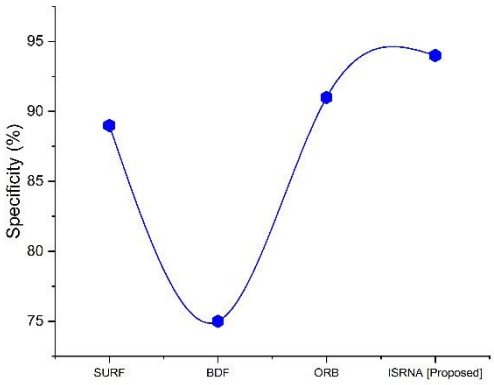

Fig.5. Specificity comparisons between the suggested and current approaches

Table 5. Comparison of Specificity

Method	**Specificity (%)**
SURF	89
BDF	75
ORB	91
ISRNA [Proposed]	94

4.5. Sensitivity

It was defined as the percentage of positives correctly identified by test out of the total number of positively significantly appraised positives. Sensitivity is a statistic employed to assess the effectiveness of CMFD algorithms. It assesses how well the system can recognize modified areas or genuine positives. Sensitivity is determined in the context of CMFD as the proportion of accurately recognized manipulated areas (true positives) to the overall number of real manipulated regions contained in an image or dataset. Figure 6 shows the comparable values for the sensitivity measures. In table 6, the Sensitivity of the suggested method is contrasted with the existing methods. In comparison to existing methods, the suggested approach offers a high level of Sensitivity. Equation (14) describes the Sensitivity

$$Sensitivity = \frac{TP}{TP+FN} \quad (14)$$

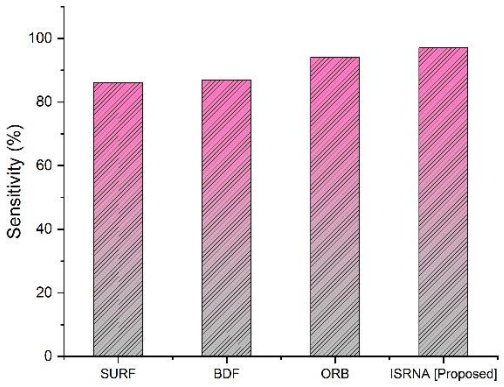

Fig.6. Sensitivity comparisons between the suggested and current approaches

Table 6. Comparison of Sensitivity

Method	**Sensitivity (%)**
SURF	86
BDF	87
ORB	94
ISRNA [Proposed]	97

5. Conclusion and Future Work

In conclusion, the CMFD in videos is a complex and evolving field. While various techniques and algorithms have been developed, further advancements are necessary to enhance accuracy, robustness, and efficiency. Continuous research and collaboration among experts in digital forensics and multimedia analysis are important to staying ahead of emerging CMF threats and ensuring the integrity of video content. In the area of artificial intelligence or related disciplines, the phrase ISRNA does not seem to be a commonly accepted or established idea. The effectiveness of the recommended strategy is shown through comparison and contrast with more conventional approaches. As a result, we introduced an integrated stochastic random neighbouring approach (ISRNA) for categorizing videos. Performance metrics like accuracy, precision, F-measure, Specificity, and sensitivity are evaluated and compared with existing technologies like the Binary Discriminative Feature (BDF), Speeded Up Robust Feature (SURF), and Oriented FAST and rotated BRIEF (OFB). The ISRNA technique combines the benefits of stochastic modelling with random Neighbor sampling in an effective and flexible approach and more effectively convergence, flexibility, resource efficiency, tolerance to noise, and scalability are just a few of its benefits. It also has a better exploration-exploitation balance. These

characteristics make it a useful tool for several applications that call for optimization, simulation, or data analysis. To improve performance, even more creative approaches might be applied to the suggested system in further studies.

References

[1] Chalamalasetty, S. P., & Giduturi, S. R. (2021). Research perception towards copy-move image forgery detection: challenges and future directions. International Journal of Image and Graphics, 21(04), 2150054.

[2] Jaiswal, A. K., & Srivastava, R. (2022). Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model. Neural Processing Letters, 54(1), 75-100.

[3] Suresh, G., & Rao, C. S. (2020). Copy move forgery detection through differential excitation component-based texture features. International Journal of Digital Crime and Forensics (IJDCF), 12(3), 27-44.

[4] Gajjar, P., Saxena, A., Shah, H., Kikani, N., Lakhani, K., Shah, P., & Limbachiya, K. (2022, August). Copy Move Forgery Detection: The Current Implications and Contemporary Practices. In Journal of Physics: Conference Series (Vol. 2325, No. 1, p. 012050). IOP Publishing.

[5] Raskar, P. S., & Shah, S. K. (2022). VFDHSOG: Copy-Move Video Forgery Detection Using Histogram of Second Order Gradients. Wireless Personal Communications, 122(2), 1617-1654.

[6] Gayathri, K. S., & Deepthi, P. S. AN OVERVIEW OF COPY MOVE FORGERY DETECTION APPROACHES.

[7] Vyas, A. ., & Sharma, D. A. . (2020). Deep Learning-Based Mango Leaf Detection by Pre-Processing and Segmentation Techniques. Research Journal of Computer Systems and Engineering, 1(1), 11–16. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/18

[8] Vijayakumar, P., Ahamed, S. B., Anitha, N., Yuvaraj, R., Gulati, K., & Kshirsagar, P. R. (2022, May). Machine learning algorithm for improving the efficiency of forgery detection. In AIP Conference Proceedings (Vol. 2393, No. 1). AIP Publishing.

[9] Armas Vega, E. A., González Fernández, E., Sandoval Orozco, A. L., & García Villalba, L. J. (2021). Copy-move forgery detection technique based on discrete cosine transform blocks features. Neural Computing and Applications, 33, 4713-4727.

[10] Jaiswal, A. K., & Srivastava, R. (2022). Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model. Neural Processing Letters, 54(1), 75-100.

[11] Elaskily, M. A., Elnemr, H. A., Sedik, A., Dessouky, M. M., El Banby, G. M., Elshakankiry, O. A., ... & Abd El-Samie, F. E. (2020). A novel deep learning framework for copy-moveforgery detection in images. Multimedia Tools and Applications, 79, 19167-19192.

[12] KOSHY, L., & SHYRY, P. (2023). Detection of Copy Move Forgery Using Rootsift and Feature Point Matching.

[13] Dhiman, O. ., & Sharma, D. A. . (2020). Detection of Gliomas in Spinal Cord Using U-Net++ Segmentation with Xg Boost Classification. Research Journal of Computer Systems and Engineering, 1(1), 17–22. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/20

[14] Aparicio-Díaz, E., Cumplido, R., Pérez Gort, M. L., & Feregrino-Uribe, C. (2019). Temporal copy-move forgery detection and localization using block correlation matrix. Journal of Intelligent & Fuzzy Systems, 36(5), 5023-5035.

[15] Abiodun, O. I., Alawida, M., Omolara, A. E., & Alabdulatif, A. (2022). Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. Journal of King Saud University-Computer and Information Sciences.

[16] Nehe, M. K. S., Birajdar, M. S. R., Ugale, M. M. K., Ugale, S. S., & Shedge, M. K. N. (2019). Framework for Image Forgery Detection. Framework, 6(11).

[17] Yang, J., Liang, Z., Gan, Y., & Zhong, J. (2021). A novel copy-move forgery detection algorithm via two-stage filtering. Digital Signal Processing, 113, 103032.

[18] Allauddin Mulla, R. ., Eknath Pawar, M. ., S. Banait, S. ., N. Ajani, S. ., Pravin Borawake, M. ., & Hundekari, S. . (2023). Design and Implementation of Deep Learning Method for Disease Identification in Plant Leaf. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 278–285. https://doi.org/10.17762/ijritcc.v11i2s.6147

[19] Akbari, Y., Al Maadeed, S., Elharrouss, O., Khelifi, F., & Lawgaly, A. (2023). A New Dataset for Forged Smartphone Videos Detection: Description and Analysis. IEEE Access.

[20] Armas Vega, E. A., González Fernández, E., Sandoval Orozco, A. L., & García Villalba, L. J.

(2021). Copy-move forgery detection technique based on discrete cosine transform blocks features. Neural Computing and Applications, 33, 4713-4727.

[21] Kadam, K. D., Ahirrao, S., & Kotecha, K. (2022). Efficient approach towards detection and identification of copy move and image splicing forgeries using mask R-CNN with MobileNet V1. Computational Intelligence and Neuroscience, 2022.

[22] Singh, G., & Singh, K. (2019). Video frame and region duplication forgery detection based on correlation coefficient and coefficient of variation. Multimedia Tools and Applications, 78, 11527-11562.

[23] Al-Qershi, O. M., & Khoo, B. E. (2018). Evaluation of copy-move forgery detection: datasets and evaluation metrics. Multimedia Tools and Applications, 77, 31807-31833.