SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I2P106

Volume 11 Issue 2, 50-59, February 2024
© 2024 Seventh Sense Research Group®

Original Article

Analysis of Copy Move Forgery Detection Process by Applying Fuzzy C Means Algorithm Based on Deep Learning in Digital Image Processing

V. Parameswaran Nampoothiri[1], N. Sugitha[2]

[1]*Department of Computer Applications, Noorul Islam Centre for Higher Education, Tamilnadu, India.*
[1]*Scientist E, Centre for Development of Advanced Computing (C-DAC), Kerala, India.*
[2]*Department of Electronics and Communication Engineering, Saveetha Engineering College, Tamilnadu, India.*

[2]*Corresponding Author : sugithavinukumar@gmail.com*

Received: 28 October 2023 Revised: 03 December 2023 Accepted: 29 December 2023 Published: 02 February 2024

Abstract *- The popularity of digital photos has developed due to technological advancements in the digital environment. Image alteration has become more manageable thanks to powerful and user-friendly photo editing software programs. Therefore, there was a prerequisite to detect the forged part of the image efficiently. Hence, this work emphasizes passive forgery recognition on images tampered by the copy move method, better called Copy Move Forgery Detection (CMFD). Copy Move Forgery (CMF) was fundamentally concerned with covering or repeating one area in a picture by pasting certain regions of a similar picture. Initially, the input digital images were preprocessed through a Gaussian filter to blur the picture to decrease noise. After preprocessing, Multi-Kernel Fuzzy C-Means clustering (MKFCM) was performed to divide the images into numerous clusters to extract the features based on distinctive attributes using the SIFT method. Lastly, with the deep learning technique, the forged parts of the images were detected. The experimental analysis demonstrates that the method was efficient and robust in identifying the forged part of the digital picture, and the performance of the proposed strategy was established on numerous forged pictures.*

Keywords *- Copy Move Forgery Detection, Deep Learning, Digital, Fuzzy C-Means clustering, Gaussian filter.*

1. Introduction

Image security is a significant concern in any area that uses digital photographs. Photographs of offenders, crime scenes, biometric photos, and other pictures have long been used in forensic examination and law enforcement. Nevertheless, with the advent of sophisticated digital picture forging methods and the lower price of obtaining a higher-quality digital image, anyone could quickly change a digital picture without leaving apparent signs. As a result, digital picture forensics has become a significant field of study [1]. Digital image forging [2] creates forged pictures by modifying real content. Digital forensic approaches secure and safeguard multimedia data when the user has no prior knowledge of the material to be protected and has not performed any pre-computation on the facts related to forgery detection. The studies are based on data post-processing. As a result, digital forensic procedures are classified as blind or passive [3].

Picture renovating, picture joining, and Copy–Move Forgery (CMF) are frequent digital picture operation attacks [3]. Copy-move tampering or cloning [4] is one of the most popular forgeries, which involves choosing, copying, and thrashing sections to the picture, expanding or whacking items or portions of relevance. Embedding a replica is one of the most prevalent methods of picture counterfeiting. In those other terms, this is referred to as a copy-move attack. The embedding procedure is divided into three stages: duplicating a fragment, adjusting this segment (strength or geometric), and putting a portion to the screen region whose information was intended to be concealed from the end user [10]. One of the image editing methods to fabricate a picture is copy-move forgery [2]. Copy-move (region duplication) is a typical attack that involves copying and pasting at least one picture component onto another section of the same picture. The copy-move fraud seeks to conceal items or overemphasize an idea by replicating specific sections. This is a type of splicing assault in which elements of two or more photos are combined to generate a new one [5].

The aim of image Copy Move Forgery Detection (CMFD) is to locate certain area(s) of an image that is identical to another area(s) of the picture [2]. Copy-Move Forgery Detection (CMFD) systems have been around for decades, and the study will guide the same process: Pre-processing, wherein the CMFD algorithms convert the query picture to grayscale

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

or coloring space before processing it. Extraction Of features, a crucial step in the CMFD approaches, involves extracting features from various image areas. Feature matching employs matching characteristics to find the original, alleged forgery areas, and post-processing, which sieves out contradictory matches/outliers from matching data and utilizes the residual pixels to see the complete discovered [7].

Block segment and crucial feature-based methods were the two primary classes of CMFD [2]. The identification and choice of higher entropy areas (key points) are required for key point-based approaches [6]. The final kind of CMFs was key point-based approaches, which extract feature points from pictures using Mirror reflection Invariant Feature Transform (MIFT), Scale Invariant Feature Transform (SIFT), and Speeded Up Robust Feature (SURF) [9]. Smooth pictures were best handled using block-based models. Nevertheless, the time complexity is significant because the picture was fragmented into several overlapping chunks [6]. There are two sorts of block-based methods: Spatial Domain and Transform Domain. Pixels are dealt with explicitly in the Spatial Domain. It correlates blocks to their respective pixels. The transform domain, on the other hand, employs several transformation algorithms to identify CMFs. Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and other transform-only methods are used [9].

Transforms like the DCT, Histogram of Orientation Gradient (HOG), Principle Component Analysis (PCA), Polar Complex Exponential Transform (PCET), DWT, Signal Value Decomposition (SVD), Zernike Moment, Polar Cosine Transform (PCT) and Fourier-Mellin Transform was used to increase the efficiency of Copy Move Forgery Detection approach or geometric distortions [8].

The key study of the proposed procedure was to perceive the forgery object using a combination of FCM and DNN. Pictures were pre-processed through a Gaussian filter to blur the picture and decrease the noise. Then, MKFCM-based segmentation is performed. After segmentation, SIFT features were taken out from each cluster. Then DNN classifier attribuer the images as original or forgery. The remaining work was planned as given; section 2 elucidates the associated studies. Section 3 explains the projected DNN-based forgery detection, and the proposed methodology-based experimental analysis is provided in Section 4. Finally, the assumption part is shown in section 5.

2. Related Study

A lot of researchers have analyzed the proposed forgery detection methodology. Few studies were examined here; Mursi et al. [11] have projected an uncovering and localization of blind CM manipulation. It's a result of combining SIFT, DBSCAN, and PCA algorithms. An approach demonstrates an ability to reveal and pinpoint interfered patches of various dimensions and figures. Moreover, the technique does not necessitate prior knowledge of the image or its editing operations. Based on numerous performance measures, a comparison was made between the approach and other tampering detection methods. The strategy proved entirely accurate in detecting and localizing copy-move manipulation.

Emam et al. [12] suggested a robust region duplicate forgery detection approach using the Difference of Gaussians (DoG) operation to extract a local extreme point. DoG was chosen as a clad approximation for the Laplacian of Gaussian (LoG) since it was easier to calculate. The Multi-support Region Order-based Gradient Histogram (MROGH) parameter was used to generate descriptive features and increase matching efficiency. They evaluated the theory's resilience to state-of-the-art procedures.

Thirunavukkarasu et al. [13] established a vital process for detecting picture manipulation utilizing a Discrete Stationary Wavelet Transform (DSWT) and Multi-Dimensional Scaling (MDS). Even though a manipulated picture was indistinct, brightness changed, color lowered, and reproduced in various spots, the method reduces computing complexity by decreasing feature size and locating the interfered area more effectively. An overall tamper detection performance was better than 97 percent, with a false positive price of less than one percent, indicating that the technology will identify tampered regions more accurately than current approaches.

Dixit et al. [14] suggested detecting Copy-Move Forgery that uses the SWT, that which, unlike greatest wavelet transforms (e.g., DWT), is shift invariant and aids in establishing the resemblances, i.e., contests and divergences, i.e., noise, among blocks of picture instigated by blurring. Features collected from a picture utilizing Singular Value Decomposition (SVD) were used to describe the sections. Additionally, the work's color-based separation approach aids in achieving blur invariance. Li et al. [15] suggested a strategy for improving forgery localization accuracy by including tampering possibility mapping. They adopt two forensic methodologies, a statistical feature-based detection and a copy-move forgery detection, after which they pick and refine tampering possibility maps. Following an examination of the characteristics of possibility mapping and an evaluation of different fusion strategies. Finally, a simple but successful technique for including the tampering probability maps into the final localization.

Lee [16] has presented a method for detecting such artefacts that are both fast and effective. The modified picture was then separated into overlying fixed-size blocks, each receiving the Gabor filter. As a result, each block is represented by a Gabor magnitude image. Second, statistical characteristics were extracted from a Histogram of Oriented Gabor Magnitude (HOGM) of neighboring pixels, and decreased features were constructed for similarity assessment.

After adequate post-processing, extracted features were lexicographically sorted, and duplicate picture blocks were recognized by discovering similar pairings. A few settings were utilized to remove the incorrectly identical blocks to improve the algorithm's robustness. Fadl et al. [17] have also developed an effective process to enhance Block Matching (BM) based CMF prevention. The work's significant contribution was using Polar representation to obtain relevant attributes for each block. The primary feature was using the Fourier transform to determine the frequencies of each block. Even when the duplicated region had undergone significant picture changes like rotation, Gaussian blurring, noise addition, scaling, luminance adjustment, and JPEG compression, the approach's effectiveness was employed for identifying Copy-Move (CM) areas.

Detecting forged images is more troublesome when the altered parts are exposed to post activities, including scaling, rotation, noise, or compression. Another difficulty in copy-move forgery recognition is that copied blocks were from similar pictures, so they possess similar properties, thus making them difficult to detect. Yet, at the same time, many issues are involved in identifying those images. Therefore, the absence of solutions to the abovementioned challenges has sparked an interest in researching this area.

3. Proposed CMF Identification Method

CMIF replicates a designated region of an image by copying and placing it in a specific section of the same image. This process of forgery is carried out to enhance the visual appeal of the image or create false evidence that appears genuine.

(a)

(b)

Fig. 1 (a) Real pictures, and (b) Forged images (copy, move, and deleted).

If Copy-Move Forgeries become prevalent in society, it will pose a significant risk to major industries such as medicine, law, education, e-commerce, and agriculture. Conventional approaches to detect forgery lack effectiveness as they fail to accurately identify the operational errors in manipulated images, whether through copy-move or splice techniques. The example in Figure 1 assumes the use of manipulated images created by executing copy, move, and delete operations.

The main objectives of the projected CMFD procedure were to develop a robust, computationally less complex, and efficient method that is very effective for blurring, noise addition, scaling, and rotational effects. Therefore, in this work, the robust method for copy moves forgery recognition depends on a deep learning algorithm, which is developed.

The projected Copy Move Forgery recognition technique has three primary stages: pre-processing, clustering, and DNN-based prediction. During the pre-processing stage, the input RGB color image was converted to a grayscale image and then filtered using Gaussian filtering. Subsequently, the image was classified into clusters by employing the MKFCM technique, which relies on the intensity of pixels.

Following the clustering process, the clustered images undergo feature extraction, in which the distinctive characteristic features of the images are extracted using the Scale Invariant Feature Transform (SIFT) method. The outliers are detected by utilizing the characteristics and employing the Deep Learning algorithm to accurately forecast the manipulated portion of an image. Figure 2 provides a schematic representation of the projected CMF recognition algorithm.

3.1. Preprocessing

Initially, the image is in the preprocessing stage. For preprocessing, 2-D Gaussian Filters (GF) were utilized. The 2D GF was frequently assumed in multi-scale edge recognition methods for the following three explanations:

- The 2D GF was the only filter that didn't generate false boundaries as the scale rises when combined with a Laplacian operator.
- The GF provides the best tradeoff among localization in both spatial and frequency-based areas.
- GF were the only rotationally invariant 2D-based filters that made the convolution in the aspatial domain very efficient, which were distinguishable in horizontal and vertical ways.

The MarrHildreth and canny detectors are two well-known edge detection methods that employ Gaussian smoothing. While Gaussian filters are most usually associated with corner detection, they are also utilized in various other uses, such as picture mosaicking and tone-based plotting of higher energetic ranging pictures.

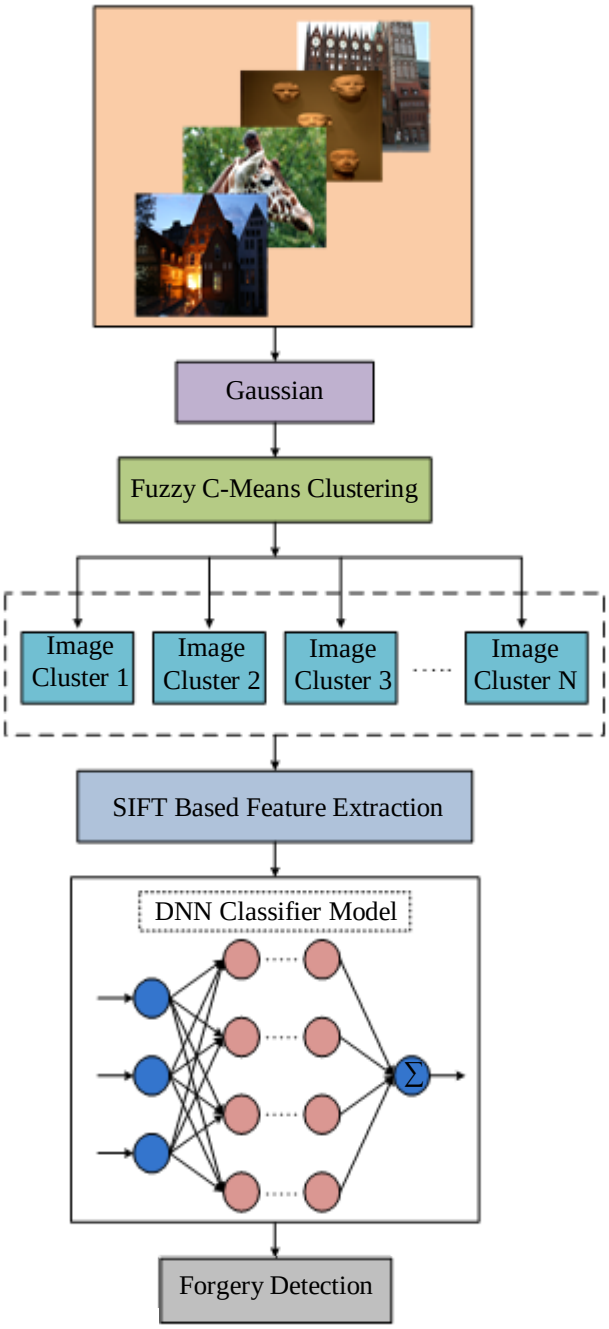

Fig. 2 Block illustration for the proposed technique

The following equations can be used to define a 2D GF positioned at the source by such a Standard Deviation (SD):

$$j(y,x)=\frac{1}{\sigma\sqrt{2\pi}}e^{\frac{-\left(y^2+x^2\right)}{2\sigma^2}} \quad (1)$$

While the function hypothetically assesses to non-zero for all values of *y* and *x*, it was a communal repetition to study the function as an efficiently 0 for y and x values elsewhere 3 SDs from the mean.

When an image i = smoothed via the GF by impulse reaction j, the smoothened image *f* originates in a frequency area by the given equation,

$$F(v,w)=I(v,w)\times J(v,w) \quad (2)$$

Where, *F(v, w), I(v, w)* and *J(v, w)* were the frequency area illustrations of *f(y, x), i(y, x),* and *j(y, x).*

Likewise, the smoothed picture may be identified in the spatial domain utilizing the convolution expression.

$$f(y,x)=i(y,x)*j(y,x) \quad (3)$$

The impulse reaction of a 2D GF should be represented via a finite quantity of parameters, often called convolution kernel or the masks, to calculate the convolution sum illustrated directly above accurately. The SD of the Gaussian function is frequently used to estimate the mask's sizes. The significant rate should be selected for smoothing, and a greater kernel was required to signify the function precisely.

3.2. Multi-Kernel Fuzzy C-Means Clustering (MKFCM)

After the preprocessing stage, the images are clustered using the MKFCM algorithm, which extends the fuzzy c-means algorithm. The gathering process was employed to find the location of the forgery detection. Given several groups c, MKFCM partitions the data X ={x1, x2,…, xn} to c fuzzy groups through minimalizing the inside cluster sum of squared error.

$$F_M=\sum_{i=1}^{c}\sum_{k=1}^{n}\left(U_{ik}\right)^m\left\|\Phi_{com}(x_k)-v_i\right\|^2 \quad (4)$$

Where;

C - Number of clusters,
N - Number of data points,
U_{ik} - Corresponding fuzzy membership function of x_k in class *i*,
m - Degree of fuzziness of the algorithm,

V = (v_1, v_2, …., v_c) represents a matrix of unidentified cluster centers (prototypes) $v_i \in R^P$, ‖●‖ characterizes the Euclidean norm.

To abridge Equation (4), the membership function and centroid are employed, which are effectively furnished in the following Equations (5), and (6).

$$c_j=\frac{\sum_{j=1}^{n}u_{ij}K_H(x_k,c_i)x_k}{\sum_{j=1}^{n}u_{ij}K_H(x_k,c_i)} \quad (5)$$

$$K_H(x_k, c_i) = K_1(x_k, c_i) + K_2(x_k, c_i) \quad (6)$$

Where,

$K_1(x_j, c_i)$ - Linear kernel

$K_2(x_j, c_i)$ - Quadratic kernel

After the MKFCM process, the number of groups is obtained. The grouped outputs were given for further processing.

3.3. Feature Extraction

After clustering, the Scale Invariant Feature Transform feature (SIFT) for each clustered image will be extracted. His feature is used for removing distinguishing invariant features from pictures. It was used a lot in image matching. The SIFT descriptor finds extreme positions over the entire image space. After feature extraction, the feature for each clustered image will be attained. Then, the extracted features were provided to DNN's input.

3.4. Deep Neural Network (DNN) Based Forgery Detection

A Deep Neural Network (DNN) is an Artificial Neural Network (ANN) consisting of multiple hidden layers between input and output. DL algorithms have high efficacy when the training phase involves many potential specimens.

In this case, the model for forging projected images was defined as a method based on DNN. During the training of a DNN, the neurons' weights were adjusted in each cycle until the difference between the output and input error fell under the specified threshold.

The operational procedure of DNN for accurately predicting the counterfeit section from the photos is divided into two distinct stages. The initial phase encompasses the training methodology, while the subsequent phase is dedicated to a testing technique.

In this context, the inputs will consist of the characteristics of the cluster groups, while the target variable will be the predetermined forged/original class labels. The DNN trains the system based on the provided information and target data. The training process is typically repeated until the suggested classifier has been confirmed using the given data.

Let $[R_m]$ = input where $1 \leq m \leq M$ and 'C' = output variable. The generalized study of the NN may be provided as 'C' for the output of the complete network and 'C_H' for the output of the hidden layer.

As in DNN, there were highly hidden layers, and the separate component inputs were reproduced through weights in the 1st hidden layer. In the concealed layer, the particular first hidden component outputs were increased by other weights, etc. In its 1st hidden layer, the weighted rates of the query were given as a summing function by the bias of a neuron (Equation (7)):

$$C_{H\_1}(x = 1,2..,K) = \left(\sum_{m=1}^{M} w_{xm} R_m \right) + b_x \quad (7)$$

Where continuous value is bias, wxm = interconnectedness weight among the input and hidden layer by representing the number of input and hidden lumps in the 1st hidden layer. The activation function, which is the output of the 1st hidden layer, was indicated as,

$$F\left(C_{H\_1}(x)\right) = \frac{1}{\left(1 + e^{-C_{H\_1}(x)}\right)} \quad (8)$$

Where,

F(.) = Sigmoid activation function

Then, the operation of Y^{th} the hidden layer can be general as,

$$C_{H\_y}(p) = \left(\sum_{z=1}^{K} w_{pz} F\left(C_{H\_(y-1)}(z)\right) \right) + b_p \quad (9)$$

Where, b_p = bias of P^{th} hidden node, w_{Pz} = interconnection weight among $(y\text{-}1)^{th}$ hidden layer and $(y)^{th}$ hidden layer with K hidden nodes. The activation function, which was the output of the Y^{th} hidden layer, was provided as,

$$F\left(C_{H\_y}(p)\right) = \frac{1}{\left(1 + e^{-C_{H\_y}(p)}\right)} \quad (10)$$

At the output layer, an output of Y^{th} the hidden layer was again reproduced by the interconnection weights (i.e., weight among the Y^{th} hidden layer and output layer) and then summed up with the bias (b_q) as,

$$C(q) = F\left(\sum_{p=1}^{K} w_{qp} \; f\left(C_{H\_y}(p)\right) + b_q \right) \quad (11)$$

Where, w_{qp} signifies the interconnectedness weight at the Y^{th} hidden layer and output layer having nodes. The initiation function at the output layer turns into an output of the whole study.

Then, the network output was compared with the target, and variance (i.e., error) was attained to improve the network output. The error design was shown in Equation (12).

$$\varepsilon = \frac{1}{M} \sum_{m=1}^{M} \left(Actual(C_m) - \Pr edicted(C_m) \right)^2 \quad (12)$$

Where, signifies projected network output and Actual (C_m) = actual output. The error should be minimal to achieve the best network structure. As a result, the weight values should be tweaked until the error is reduced at each cycle.

4. Result and Discussion

Photographs were captured as benchmarks in this study for analysis. Firstly, a preprocessing step is performed using a Gaussian filter to turn the color image into a grayscale image. Next, the Fuzzy C-means clustering technique is utilized to partition the preprocessed image into distinct clusters determined by the intensity values. Subsequently, the distinctive characteristics of the object were retrieved using the SIFT technique. Ultimately, the DNN accurately predicted a portion of the manipulated images. Matlab version (7.12) is utilized to develop the proposed approach. This method is tested on a Windows system with an Intel Core i5 processor running at 1.6 GHz and 4 GB of RAM. The suggested approach was evaluated using data sets that are freely accessible.

4.1. Estimation Metrics

The system-based performance was examined through the assessment metrics like Sensitivity, False Negative Rate (FNR), Positive Predictive Value (PPV), Specificity, Negative Predictive Value (NPV), Accuracy, False Positive Rate (FPR), and False Discovery Rate (FDR) that was portrayed as.

4.1.1. Sensitivity

The proportion of a number of True Positives (TP) to its TP sum and False Negative (FN) is known as sensitivity.

$$Sensitivity = \frac{No.of\,(TP)}{No.of\,(TP) + No.of\,(FN)} X100 \tag{13}$$

4.1.2. Specificity

Specificity is a proportion of the number of True Negative (TN) to the TN sum and False Positive (FP).

$$Specificity = \frac{No.of\,(TN)}{No.of\,(TN) + No.of\,(FP)} X100 \tag{14}$$

4.1.3. Accuracy

Accuracy is evaluated through the actions of sensitivity and specificity. It was signified as given,

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} X100 \tag{15}$$

4.1.4. PPV

The portion of positive trial consequences that were measured as the PPV.

$$PPV = \frac{TP}{TP + FP} \tag{16}$$

4.1.5. NPV

The portion of negative experimentation significances that were measured as the NPV:

$$NPV = \frac{TN}{TN + FN} \tag{17}$$

4.1.6. FPR

FPR is premeditated as the number of inappropriate optimistic forecasts categorized through the total number of negatives. It could be evaluated as 1 – specificity.

$$FPR = \frac{FP}{FP + TN} \tag{18}$$

4.1.7. FNR

FNR was designed as the number of improper negative forecasts separated by the total number of negatives.

$$FNR = \frac{FN}{FN + TP} \tag{19}$$

4.1.8. FDR

FDR, a rate that features named influential, was truly empty that was described as.

$$FDR = \frac{FP}{FP + TP} \tag{20}$$

4.2. Performance Evaluation

The fundamental idea of the suggested technique involved the prediction of counterfeit sections within the input digital images through the utilization of various stages. The performance was assessed using multiple metrics. This effort consists of two crucial stages: segmentation and classification.

This analysis examines the performance of the predicted MKFCM and the existing K-means and FCM approaches in this sector. Integrating the DL algorithm with the MKFCM approach is proposed to identify fabricated portions of an image and produce an effective detector for digital image forgery. The following graphic displays some of the analyzed input database digital photographs.

Figure 3 compares the original digital image, the duplicated image, and a specific area of the copied image that has been segmented. The proposed process involved capturing and segmenting pictures from the original digital picture. Therefore, to examine the counterfeit portion of the digital image.

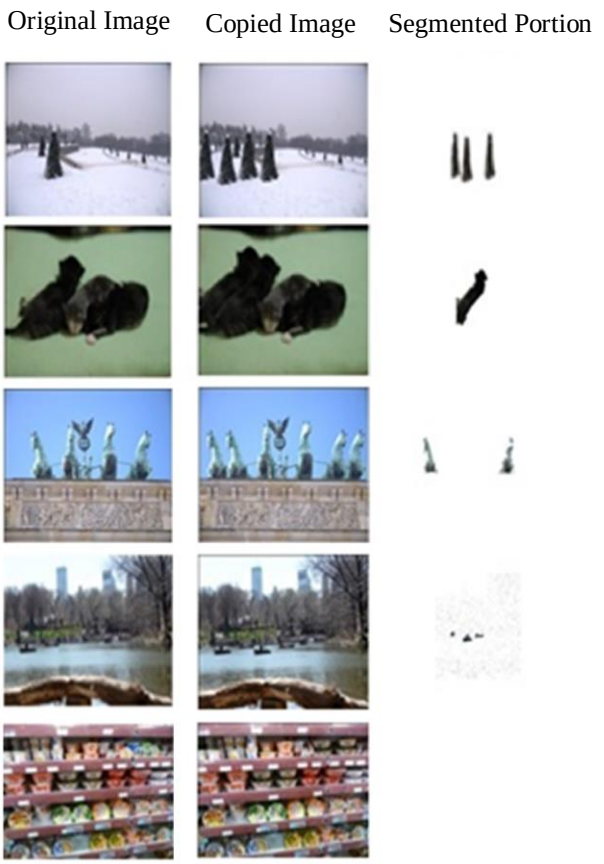

Fig. 3 Segmentation results

Tables 1, 2, and 3 display the performance metrics of the proposed and existing techniques. The following measurements were utilized: FNR, PPV, NPV, FPR, sensitivity, FDR, accuracy, and specificity. For analysis, a total of five sets of digital photographs were captured.

The input images were analyzed by clustering and extracting features for the forged component and segmented part of the original image. The sensitivity measures obtained for image 1 are 0.99656, 0.9312, and 0.94126 for MKFCM, K-Means, and FCM, respectively. Similarly, in terms of precision, the suggested method achieved a specificity of 0.99601 and an accuracy of 0.98605. Therefore, based on the analysis of all metrics, it is evident that the proposed MKFCM technique outperforms the existing K-means and FCM methods. The graph below presents a comprehensive visual depiction of proposed and existing techniques.

Upon examining Figures 4 to 6, it is evident that the proposed strategy accomplishes the desired outcome. Therefore, the proposed method surpasses the known techniques. This research employs a deep-learning neural network to detect forgeries. This research presents the experimental findings from categorizing forgery detection using a DNN.

To demonstrate the effectiveness of the algorithm, we compared the proposed DNN-based classification with other algorithms, including the Random Forest (RF), the K-Nearest Neighbour classifier (KNN), and the Artificial Neural Network (ANN). The performances are evaluated based on the metrics. i.e., FPR, sensitivity, NPV, accuracy, PPV, specificity, and FNR.

The classification stage yields the experimental outcome, which is presented in Table 4. Upon examining Table 4, it is evident that the suggested DNN-based forgery detection technique achieved a maximum precision of 93%. This result surpasses the performance of other forgery detection methods, such as KNN, RF, and ANN, by 28.23%, 37.7%, and 37.7%, respectively. DNN has successfully addressed the challenges that exist in previous methods. Likewise, the highest level of sensitivity and specificity is achieved. Additionally, the table included a discussion on the NPV, PPV, FNR, and FPR. The proposed strategy yields the highest outcomes when compared to results obtained using other methods.

Table 1. Accuracy, specificity, and sensitivity evaluation metrics

Image Name	Sensitivity			Specificity			Accuracy		
	MKFCM	**FCM**	**K-Means**	**MKFCM**	**FCM**	**K-Means**	**MKFCM**	**FCM**	**K-Means**
Image 1	**0.995656**	0.94217	0.9211	**0.99769**	0.98958	0.9865	**0.98768**	0.97497	0.96589
Image 2	**0.97636**	0.89195	0.8734	**0.99899**	0.98396	0.9654	**0.98754**	0.97165	0.96145
Image 3	**0.97769**	0.83200	0.7289	**0.99563**	0.97895	0.9833	**0.98634**	0.97121	0.96148
Image 4	**0.97832**	0.93210	0.8748	**0.99986**	0.97852	0.9769	**0.98853**	0.97760	0.96759
Image 5	**0.97209**	0.87499	0.7697	**0.99795**	0.97847	0.9801	**0.98684**	0.97542	0.96384

Table 2. PPV, NPV, and FPR evaluation metrics

Image Name	PPV			NPV			FPR		
	MKFCM	FCM	K-Means	MKFCM	FCM	K-Means	MKFCM	FCM	K-Means
Image 1	0.94578	**0.9932**	0.993	**0.99876**	0.9943	0.999	**0.00398**	0.0004	0.0002
Image 2	0.99683	**1.1001**	1.001	**0.99722**	0.9882	0.983	0.00024	**0.0000**	0.0000
Image 3	0.91142	**0.9345**	0.993	**0.99843**	0.9911	0.991	0.00352	**0.0002**	0.0002
Image 4	0.83194	**0.9543**	0.971	**0.99879**	0.9982	0.998	0.00147	**0.0001**	0.0003
Image 5	0.93345	**0.9954**	0.993	**0.99854**	0.9955	0.993	0.00153	**0.0002**	0.0002

Table 3. FNR and FDR evaluation metrics

Image Name	FNR			FDR		
	MKFCM	FCM	K-Means	MKFCM	FCM	K-Means
Image 1	**0.00333**	0.0690	0.070	**0.05219**	0.0059	0.004
Image 2	**0.01483**	0.1169	0.120	**0.00279**	0.0000	0.000
Image 3	**0.02112**	0.2679	0.270	**0.08739**	0.0052	0.004
Image 4	**0.02080**	0.1190	0.121	**0.16929**	0.0298	0.028
Image 5	**0.02869**	0.2239	0.230	**0.06330**	0.0070	0.006

Table 4. Performance based on the classification stage

Methods	Accuracy	Sensitivity	Specificity	PPV	NPV	FPR	FNR
DNN	**0.93**	**0.94**	**0.94**	**0.9729**	**0.6925**	**0.1**	**0.1**
KNN	0.725	0.4	0.66	0.8356	0.2565	0.5	0.264
RF	0.675	0.4	0.62	0.8282	0.2451	0.5	0.334
ANN	0.675	0.5	0.64	0.8535	0.2676	0.6	0.334

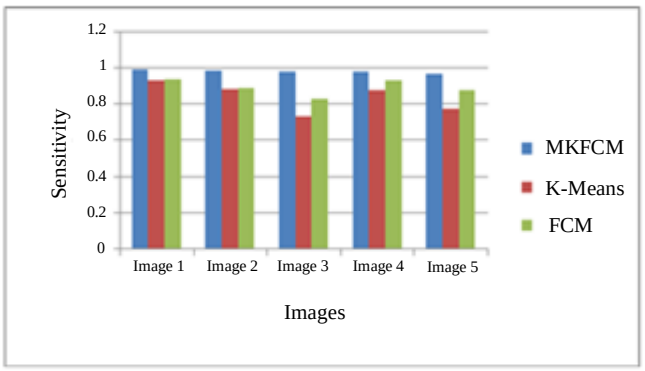

Fig. 4 Quantification of the sensitivity of existing and proposed methods

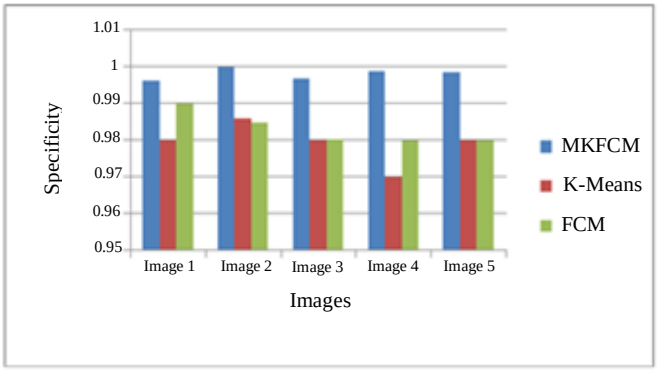

Fig. 5 Comparative analysis of the FCM and K-means algorithms in terms of the specificity metric

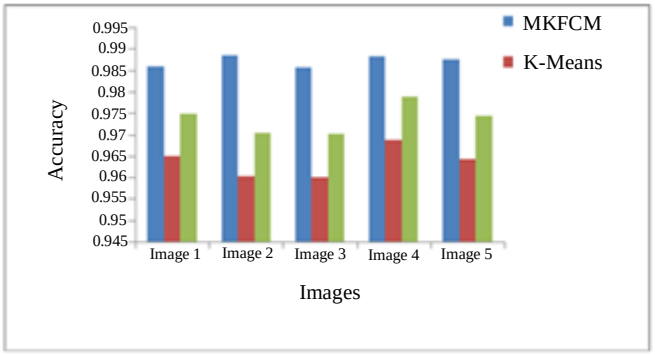

Fig. 6 Calculation of accuracy for existing and proposed methods

4.3. Comparison Study

To verify the efficiency of the proposed procedure, a comparison of the projected methodology with already published work is necessary. For analysis, four existing works are utilized. In Amerini et al. [18], CMF identification and localization regarding strong gathering by J-Linkage is proposed. In Cozzolino et al. [19], patch match detection-based CMF identification was presented. This works based on block-based features. Cozzolino et al. [20] introduced Circular Harmonic Transforms (CHT) and PatchMatch-based forgery detection. Similarly, in Xiang et al. [21], key-point-based CMFD for color pictures was anticipated. Methods are given good results. Even though it should be maximizing the result. So, in this work, cluttering with DNN is proposed for forgery detection.

The demonstration of a projected technique was examined relative to the F-measure. Figure 7 exemplifies the proposed technique's resilience regarding the F-measure cure. The suggested CMFD technique performs better than all comparison references, as shown in Figure 7, with a performance benefit becoming quite considerable in the ideal situation and under varied assaults.

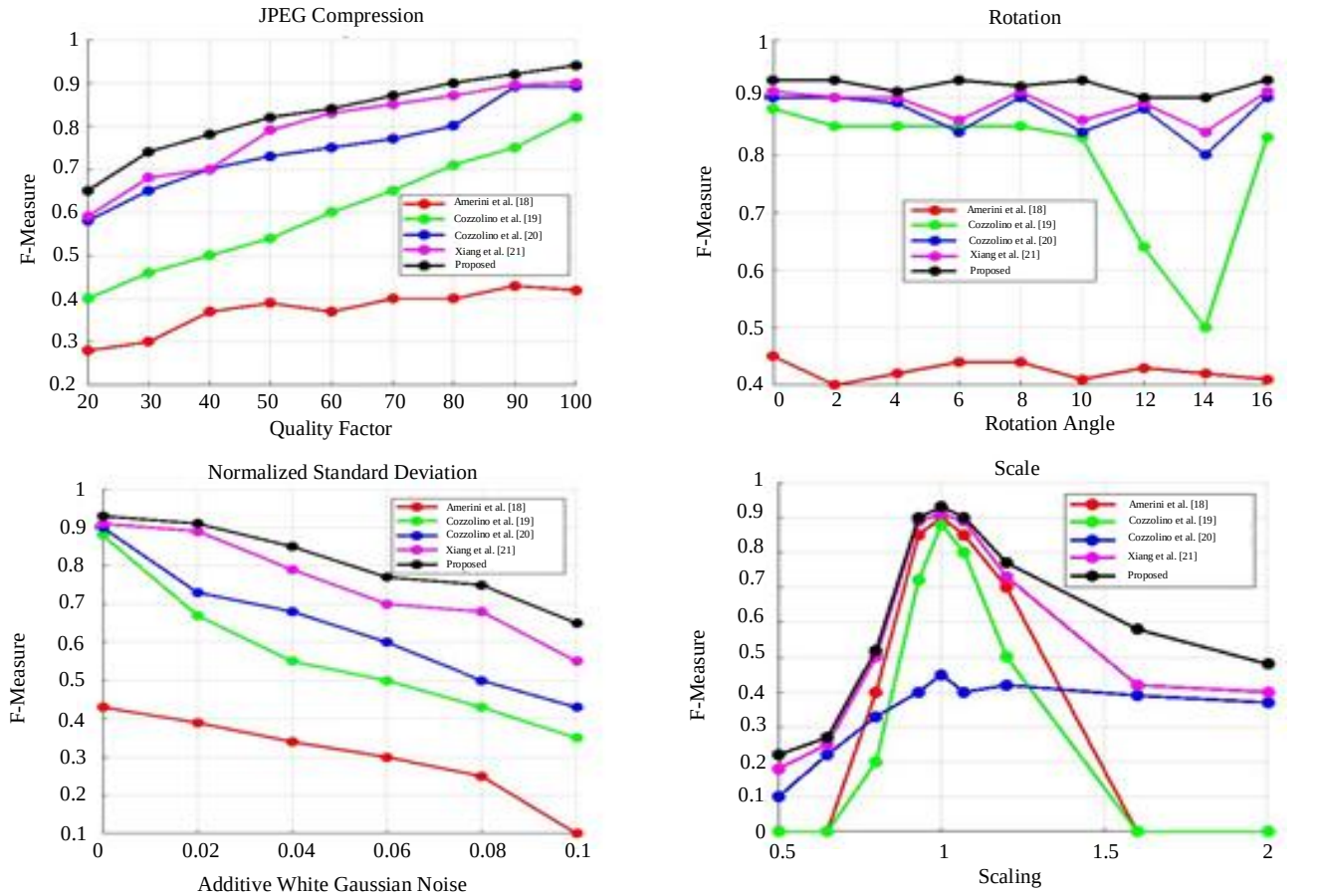

Fig. 7 F-measure curves for several CMFD approaches. Four image processing techniques are (a) JPEG compression, (b) Rotation, (c) Additive white Gaussian noise, and (d) Scaling.

5. Conclusion

This article presents a novel approach for detecting forgeries, utilizing a process called CMFD with a DL algorithm based on Fuzzy C-Means clustering. The initial digital photos are processed in the preprocessing stage using a Gaussian filter, converting RGB color images into grayscale images. Next to preprocessing, the Fuzzy C-means gathering method was run to partition the preprocessed images into

multiple clusters. Next, the distinctive characteristics of the object are obtained using the SIFT technique. Finally, a DNN was utilized to forecast the counterfeit portion of the image. The approach for identifying planned copy-move forgeries was implemented in the MATLAB working platform. It is also calculated using various presenting metrics like sensitivity, PPV, specificity, NPV, FPR, FNR, and FDR. It was observed that the anticipated technique outperforms improved than the existing approaches. In the future, an optimization algorithm to enhance the performance of the proposed methodology will be introduced.

References

[1] Shi Wenchang et al., "Improving Image Copy-Move Forgery Detection with Particle Swarm Optimization Techniques," *China Communications*, vol. 13, no. 1, pp. 139-149, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[2] Badal Soni, Pradip K. Das, and Dalton Meitei Thounaojam, "CMFD: A Detailed Review of Block Based and Key Feature Based Techniques in Image Copy-Move Forgery Detection," *IET Image Processing*, vol. 12, no. 2, pp. 167-178, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[3] Rahul Dixit, and Ruchira Naskar, "Review, Analysis and Parameterisation of Techniques for Copy-Move Forgery Detection in Digital Images," *IET Image Processing*, vol. 11, no. 9, pp. 746-759, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[4] Anselmo Ferreira et al., "Behavior Knowledge Space-Based Fusion for Copy-Move Forgery Detection," *IEEE Transactions on Image Processing*, vol. 25, no. 10, pp. 4729-4742, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mohsen Zandi, Ahmad Mahmoudi-Aznaveh, and Alireza Talebpour, "Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2499-2512, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[6] Yan Wo et al., "Copy-Move Forgery Detection Based on Multi-Radius PCET," *IET Image Processing*, vol. 11, no. 2, pp. 99-108, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[7] Xiuli Bi, and Chi-Man Pun, "Fast Copy-Move Forgery Detection Using Local Bidirectional Coherency Error Refinement," *Pattern Recognition*, vol. 81, pp. 161-175, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[8] Xiuli Bi, and Pun Chi-Man, "Fast Reflective Offset-Guided Searching Method for Copy-Move Forgery Detection," *Information Sciences*, vol. 418-419, pp. 531-545, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[9] Devanshi Chauhan et al., "Survey on Keypoint Based Copy-Move Forgery Detection Methods on Image," *Procedia Computer Science*, vol. 85, pp. 206-212, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[10] Andrey Kuznetsov, and Vladislav Myasnikov, "A New Copy-Move Forgery Detection Algorithm Using Image Preprocessing Procedure," *Procedia Engineering*, vol. 201, pp. 436-444, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[11] Mona F. Mohamed Mursi, May M. Salama, and Mohamed H. Habeb, "An Improved SIFT-PCA-Based Copy-Move Image Forgery Detection Method," *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, vol. 6, no. 3, pp. 23-28, 2017. [Google Scholar]

[12] Mahmoud Emam et al., "A Robust Detection Algorithm for Image Copy-Move Forgery in Smooth Regions," *2017 International Conference on Circuits, System and Simulation (ICCSS)*, London, UK, pp. 119-123, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[13] V. Thirunavukkarasu et al., "Nonintrusive Forensic Detection Method Using DSWT with Reduced Feature Set for Copy-Move Image Tampering," *Wireless Personal Communications*, vol. 98, pp. 3039-3057, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[14] Rahul Dixit, Ruchira Naskar, and Swati Mishra, "Blur-Invariant Copy-Move Forgery Detection Technique with Improved Detection Accuracy Utilising SWT-SVD," *IET Image Processing*, vol. 11, no. 5, pp. 301-309, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[15] Haodong Li et al., "Image Forgery Localization via Integrating Tampering Possibility Maps," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1240-1252, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[16] Jen-Chun Lee, "Copy-Move Image Forgery Detection Based on Gabor Magnitude," *Journal of Visual Communication and Image Representation*, vol. 31, pp. 320-334, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[17] Sondos M. Fadl, and Noura A. Semary, "Robust Copy-Move Forgery Revealing in Digital Images Using Polar Coordinate System," *Neurocomputing*, vol. 265, pp. 57-65, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[18] Irene Amerini et al., "Copy-Move Forgery Detection and Localization by Means of Robust Clustering with J-Linkage," *Signal Processing: Image Communication*, vol. 28, no. 6, pp. 659-669, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[19] Davide Cozzolino, Giovanni Poggi, and Luisa Verdoliva, "Copy-Move Forgery Detection Based on Patchmatch," *2014 IEEE International Conference on Image Processing (ICIP)*, Paris, France, pp. 5312-5316, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[20] Davide Cozzolino, Giovanni Poggi, and Luisa Verdoliva, "Efficient Dense-Field Copy-Move Forgery Detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2284-2297, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[21] Xiang-Yang Wang et al., "A New Keypoint-Based Copy-Move Forgery Detection for Small Smooth Regions," *Multimedia Tools and Applications*, vol. 76, pp. 23353-23382, 2017. [CrossRef] [Google Scholar] [Publisher Link]