Analysis of Copy Move Forgery Detection Process Using Fuzzy C Means Based Deep Learning Algorithm in Digital Image

Parameswaran Nampoothiri (nampoothirip605@gmail.com)  
C-DAC Thiruvananthapuram

Sugitha N  
NICHE Kumaracoil

Research Article

Keywords: Deep Learning, Copy Move Forgery Detection, Fuzzy C-means clustering, SIFT, Gaussian filter

Posted Date: July 22nd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-499456/v1

License: © This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
Analysis of Copy Move Forgery Detection Process Using Fuzzy C Means Based Deep Learning Algorithm in Digital Image

*1 Parameswaran Nampoothiri V, *2 Dr. N Sugitha

*1 Principal Engineer, CDAC, Thiruvananthapuram

*2 Associate Professor, NICHE, Kumaracoil

Gmail: nampoothirip605@gmail.com

Abstract

Technological advances in the digital world have led to a tremendous growth in the popularity of digital photography in all walks of life. However, photo editing software tools are easy to use and make photo manipulation a breeze. Therefore, there is a need to find the wrong part of the image. Therefore, this work focuses on finding false images used using the copying process, better known as Copy Move Forgery Detection (CMFD). A copy of Motof spoofing basically means to hide or duplicate a place in a region by attaching certain parts of the same image to it. Initially, digital input images are pre-processed with a Gaussian filter, which is used to blur the image and reduce noise. After further development, a collection of Multi-kernel Fuzzy C-means clustering (MKFCM) was developed to classify images into multiple groups and depending on the various features, the features were extracted using the SIFT algorithm. Finally, with the help of an in-depth reading method, part of the illegal images are found. Test results show that this method is effective and efficient in detecting digital image deception and its functionality and the proposed method is shown in false images.

Keywords: Deep Learning, Copy Move Forgery Detection, Fuzzy C-means clustering, SIFT, Gaussian filter.
1. Introduction

Photographic security is an important issue in any field that allows us to have digital photography. Photographs have long been a part of judicial investigations and law enforcement, for example crime photographs, crime scenes, biometric photographs, etc. However, with the advent of basic digital imaging techniques and the low cost of obtaining high-quality digital images, anyone can easily use digital images without leaving visible fingerprints. Therefore, forensic analysis of digital images has become an important field of investigation [1]. The creation of embedded images with misleading image content is called digital imaging [2]. Digital forensic techniques provide security and protection for multimedia data when the user does not have to protect the data and the data was not pre-calculated before the forgery was detected. The research is based on the use of data. Therefore, digital forensic techniques fall into the category of blind or artificial [3].

The most common types of digital photo editing attacks include image reloading, image cropping, and copying and animation. Other common formats include image-based area selection, copy and paste objects, copy or hide objects or parts of interest, copy / paste, use processes, or merge. [4]. One of the most common ways to create images is to embed duplicates. In other words, this attack is called copying. The embedding process consists of three stages: copying a clip, inserting changes (transforming power or geometry) into a clip and inserting a clip into that part of the image whose content will be hidden from the end user [10]. Copying and pasting lies is one of the many ways to use an image to deceive an image [2]. Copy movement (regional duplication) is a common attack when at least one part of an image is copied and pasted into another part of the same image. The main purposes of counterfeit copy and movement to
conceal or impress an idea by imitating other regions. This is a special case of splice attack (parts of two or more images combined to create a new one) [5].

Acquisition of a copy move forgery detection (CMFD) to obtain other regions similar to other regions of the image as the copied part is copied to the same image [2]. Decades ago, CMFD copying methods often followed a standard procedure: initial analysis, in which CMFD methods first converted an image to gray in color or color space, the main CMFD phase methods, in which different regions were extracted, including the acquisition of related functions, suspicious and background filters, incompatible or inconsistent with using the remaining pixels to obtain final results [7].

CMFD can be classified into two main categories: block segregation and mechanisms designed to act [2]. Selection-based approaches are based on the identification and selection of an area of high entropy (key points) [6]. The latter type uses key-based methods where SIFT (Scale Invariable Entity Transformation), MIFT (Mirror Reflection Invariable Entity Transformation), and SURF (Robust Acceleration Function) are used to extract image points from images [9]. Block method based images are great for dealing with those smooth images. However, the time constraints are high as the image is divided into many different blocks [6]. The block-based approach is divided into two categories: spatial domain and transformation domain. Spatial Domain works directly with pixels. Compare the blocks to your pixel. Another type is a conversion platform where various conversion methods are used to get a fake copy. Just change the method, use DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform), etc. [9].

Improved efficiency of writing methods, modifications such as Discrete Cosine Transform (DCT), Principle Component Analysis (PCA), Discrete Wavelet Transform (DWT),
Signal Value Decomposition (SVD), Histogram of Orientation Gradient (HOG), Zernike Moment, Fourier-Mellin Transform, Polar Complex Exponential Transform (PCET), and Polar Cosine Transform (PCT) have been used to eliminate intangibles by standard deviation or distortion. Geometry. [8].

The main objective of this proposed method is to detect counterfeit material using a combination of FCM and DNN. Images are first processed with a Gaussian filter to blur the image and reduce noise. After that, the MKFCM based separation was performed. After dividing, the SIFT functions are released in each group. After that, based on characteristics, DNN classification classifies images as original or non-original. Some of the tasks are listed as such, section 2 describes related activities. Section 3 describes the DNN-based fraudulent discovery and the results of the proposed test are provided in section 4. Finally, the final phase is entered in section 5.

2. Related Work

A large number of researchers are analyzing the proposed method to identify fraud. Among them some of the works are analyzed here; Mursi et al. [11] suggested how to detect and detect blind movement and the use of copies. According to strategic agreements SIFT, PCA and DBSCAN. This method demonstrates your ability to produce and obtain used circuits of different sizes and sizes. Furthermore, this method does not require prior details about the image or deceptive actions performed on it. Comparative analysis between other disturbance modalities was evaluated according to various operational measures. Her method was reliable to obtain and acquire the movement and conversion of copies.

Emam et al. [12] suggested a method for obtaining strong regional duplication based on the issuance of local points from a Difference of Gaussians (DoG). The dose was used because
it was a good laparoscopy of Laplacian of Gaussian (LoG) and was very quick to calculate. In order to extract descriptive features and thus continuously improve performance, the definition of the gradient histogram was defined on the basis of the Multi-support Region Order-based Gradient Histogram (MROGH). The robustness of the method was compared with the new production methods.

Thirunavukkarasu et al. [13] performed a rigorous process using Discrete Standing Wave Transform and Multidimensional Scaling to obtain a contradictory image. This method reduces the difficulty of calculation by reducing the size of the work and finding the distorted area accurately even if the distorted image is blurred, the light changes, the color is blurred, and is included in many areas. The accuracy of the total acquisition was greater than 97% and the negative positive was almost zero, indicating that this approach would more accurately affect the region compared to existing methods.

Dixit et al. [14] proposed a duplicate copy using stationary wavelet transform (SWT), in contrast to multiple wavelet transformers (eg, discrete wavelet transform), which were inconsistent and helped to establish similarities, that is, matches and comparisons, that is, sound, enter lock images, caused by blur. Blocks are represented by objects extracted using a singular value decomposition (SVD). Also, the concept of color separation used in the work helps to achieve blurry contrast. Li et al. [15] propose a framework to improve the performance of a simulated environment by integrating potential maps. They first select and build two forensic methods, namely a function-based detector and a typewriter, and then prepare to find disturbing maps. After investigating the potential properties of the map and comparing different integration schemes. Ultimately, a simple mapping strategy can disrupt storage availability.
Lee [16] suggested an effective and robust way to acquire that art. First, the converted image was divided into scattered blocks of dry size and a Gabor filter was applied to each block. Therefore, an image the size of Gabor represents each block. Second, statistical features were extracted from the histogram of orientated Gabor magnitude (HOGM), and reduced features were performed to measure similarity. Finally, the characteristic vectors were lexicographically separated and duplicate image blocks were found by searching in pairs of the same blocks after proper processing. To improve the durability of the algorithm, other parameters have been used to remove the same bad blocks. In addition,

Fadl et al. [17] suggested an effective way to improve Copy-Move fraud detection based on Block Matching (BM). A major contribution of this work was the use of polar representation to determine the individual characteristics of each block. The main feature used the frequency of each block in the Fourier type. Functionality of the method used to locate Copy-Move (CM) regions, even if the copied location received image variations such as rotation, scale, Gaussian size, light conversion, JPEG compression and sound enhancement.

Finding merged images becomes a major problem when converted parts are made to send tasks such as scale, rotation, sound or compression. Another problem with receiving a copy of a fake post is that the copied blocks are from the same image and therefore have the same properties, making it harder to find. But at the same time, it is a great pleasure to see those pictures. Therefore, the lack of solutions to the above means problems that have encouraged research in this area.
3. Proposed copy-move forgery detection method

Copy-Move image forgery is duplicating the particular region of an image by pasting it in certain portion of the same image. This forgery is done to make the image more pleasant or produce the pseudo proof for appearance. Some important fields like medical, law, education, e-commerce, agriculture etc. will be under risk if the copy-move forgery plays vital role in the society. Bench marked images which are forged by performing Copy, Move and Delete operations are given in the below example figure 1.

![Original Images](a) (b) (c) : Original Images; (d) (e) (f) : Forged Images (Copy, Move and Deleted)

Figure 1: (a) (b) (c) : Original Images; (d) (e) (f) : Forged Images (Copy, Move and Deleted)

The main objectives of the proposed writing style are to create a robust, integrated and efficient system of active shading, sound input, measurement effects and rotation. Therefore, this project has provided a solid way to obtain a copy of the Deep Learning algorithm. The proposed method of obtaining a counterfeit copy involves three main steps including preprocessing, compilation, and DNN-based prediction. Initially, during preprocessing, the RGB input color image is converted to grayscale and filtered using Gaussian filtering. Then the image is collected in pixel size using the MKFCM method. After fusion, the fused images are designed for feature
extraction, in which various elements of the image are extracted using SIFT (Scale Invariable Feature Transformation). Using features, outliers are identified according to the learning algorithm to accurately predict the constructed part of an image. The following figure provides a detailed diagram of how to obtain a copy of the proposed copy.

Figure 2: Block diagram for the proposed method
3.1 Preprocessing:

Initially, the image is in the pre-processing phase. Improved, using 2D Gaussian filters. Gaussian 2D filters are generally accepted for decision-making purposes for the following three reasons:

- Gaussian filters offer excellent compensation in place for both locations and domains.
- Gaussian filters are the only 2D alternating filters that enable local domain power to work, separated by direct and indirect indicators.

Among the many cutting algorithms that use Gaussian smoothing are the MarrHildreth detector and the smart detector. While Gaussian filters are widely used locally, they are also used in many other applications, including high-resolution editing and high-resolution map editing.

A 2D Gaussian work that focuses on one common deviation can be described by:

\[
j(y, x) = \frac{1}{\sigma \sqrt{2\pi}} e^{-\frac{(y^2 + x^2)}{2\sigma^2}}
\]  

(1)

While a mathematician retests the zero of all numbers, it is y and x common to assume that a function does not work with numbers and that there are more than y and x three common errors in the definition.

When the image \( i \) is smooth with a Gaussian filter with a \( j \) strong response, a smooth image \( f \) in the background can be obtained using the expression

\[
F(v, w) = I(v, w) \times J(v, w)
\]

(2)

Where \( F(v, w) \), \( I(v, w) \) and \( J(v, w) \) are respectively the frequency domain representations of \( f(y, x) \), \( i(y, x) \) and \( j(y, x) \).
\[ f(y,x) = i(y,x)^* j(y,x) \]

To accurately calculate the amount of convolution shown above, the response rate of the 2D filter \( j(y,x) \) must be measured by the estimated number of coefficients, better known as the kernel or convolution mask. The size of the mask is usually \( (\sigma) \) determined by the normal deviation of the Gaussian function. For maximum smoothness, a large number should be selected and a large grain is required to accurately represent the job.

### 3.2 Multi-kernel Fuzzy C-means clustering (MKFCM):

After the preprocessing stage, the images are clustered using MKFCM algorithm which extends the fuzzy c-means algorithm. The group process is used to identify duplicates. Given the number of clusters, MKFCM minimizes the sum of squares within the data class = \( x \{ x_1, x_2, \ldots, x_n \} \) cluster and divides them into \( C \) obscure clusters. \( C \)

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

Where:
- \( c \rightarrow \) clusters Number,
- \( n \rightarrow \) Data points Number,
- \( U_{ik} \rightarrow \) Corresponding fuzzy membership function of \( x_k \) in class \( i \),
- \( m \rightarrow \) Degree of fuzziness of the algorithm,
- \( V = (v_1, v_2, \ldots, v_c) \) represents a matrix of unidentified cluster centers (prototypes) \( v_i \in \mathbb{R}^p \),
- \( \| \cdot \| \) characterizes the Euclidean norm
\[
    c_j = \frac{\sum_{j=1}^{n} u_{ij} K_H(x_k, c_i) x_k}{\sum_{j=1}^{n} u_{ij} K_H(x_k, c_i)}
\]  
(5)

\[
    u_{ij} = \frac{(1 - K_H(x_k, c_i))^{-1/m-1}}{\sum_{k=1}^{c} (1 - K_H(x_k, c_i))^{-1/m-1}}
\]  
(6)

\[
    K_H(x_k, c_i) = K_1(x_k, c_i) + K_2(x_k, c_i)
\]  
(7)

Where;

\[K_1(x_j, c_i) \rightarrow \text{Linear kernel}\]

\[K_2(x_j, c_i) \rightarrow \text{Quadratic kernel}\]

After MKFCM process, the number of clusters is obtained. The clustered outputs are given to the further processing.

### 3.3 Feature extraction

After clustering process, the Scale Invariant Feature Transform feature (SIFT) for each clustered image will be extracted. Its feature is used to extract different elements that are different from the images. It is widely used in image comparisons. The SIFT indicator gets the last point in the space on the scale. After the feature is released, features \(1 \times n\) of each collected image will be available. Features extracted and exported to DNN entries.

### 3.4 Deep neural network (DNN) based forgery detection:

A deep neural network (DNN) is an artificial neural network (ANN) with many hidden layers of units between input and output layers. Deep learning methods are most effective when the number of samples available within the training phase is large. Here, the proposed image
manipulation model is defined in a DNN-based way. During DNN training, neurons regenerate throughout the cycle until the error between output and input is within the limit. The working procedure of DNN for forecasting the forged portion from the images is categorized into two phases. The first phase involves the training process and the second phase is involved of the testing process. Here, the inputs will be the features of the cluster groups and the Target is fixed as forged/original class labels. Based on the input and target data, the training process is done using DNN. Generally, the training process is repeated until the proposed classifier is trained with the data provided.

Let \([R_m]\) be the input where \(1 \leq m \leq M\) and 'C' be the output variable. The standard network model can be provided as "C" for all network operations and hidden extensions "\(C_H\)". Like DNN, there are many hidden layers, with duplicate insertion in the first hidden layer. Also, each output of the first hidden object is multiplied by another set of weights in the second hidden layer and so on.

\[
C_{H-1}(x = 1, 2, .., K) = \left( \sum_{m=1}^{M} w_{xm} R_m \right) + b_x \quad (8)
\]

The activation function which is the output of the first hidden layer is given as,

\[
F\left( C_{H-1}(x) \right) = \frac{1}{1 + e^{-C_{H-1}(x)}} \quad (9)
\]

Where, \(F(\cdot)\) is the sigmoid activation function

\[
C_{H-1}(p) = \sum_{z=1}^{K} w_{pz} F\left( C_{H-2}(z) \right) + b_p \quad (10)
\]
Where \( p_b \) is the bias of \( p^{th} \) hidden node, \( w_{pc} \) is the interconnection weight between the \((y-1)^{th}\) hidden layer and \((y)^{th}\) hidden layer with \( K \) hidden nodes.

The activation function which is the output of the \( y^{th} \) hidden layer is given as,

\[
F(C_{H_y}(p)) = \frac{1}{1 + e^{-C_{H_y}(p)}}
\]  

(11)

At the output layer, the output of \( y^{th} \) hidden layer is again multiplied with the interconnection weights (i.e. weight between the \( y^{th} \) hidden layer and output layer) and then summed up with the bias \( (b_q) \) as

\[
C(q) = F\left( \sum_{p=1}^{K} w_{qp} f(C_{H_y}(p)) + b_q \right)
\]

(12)

\[
\varepsilon = \frac{1}{M} \sum_{m=1}^{M} \left( Actual(C_m) - Predicted(C_m) \right)^2
\]

(13)

Where, \( Predicted(C_m) \) is the estimated network output and \( Actual(C_m) \) is the actual output.

4. Result and discussion

In the proposed work, bench marked images are taken for analyses. Initially, processing is applied with a Gaussian filter when the color image is converted to a gray scale image. Subsequently the Fuzzy C-means clustering method was developed to separate the previously created image into clusters based on price values. And then its features are released with the help of SIFT algorithm to extract various features. Finally, using the Deep Neural Network, part of the images were predicted. Using the proposed procedure, the Matt lab type (7.12) is used. This proposed method is performed on a windows machine with an Intel Core 5 processor at a speed
of 1.6 GHz and 4 GB of RAM. The proposed system has been tested on public data sets on the web.

4.1. Evaluation metrics

The system performance is analyzed by using the assessment metrics such as Sensitivity, Specificity, Accuracy, Positive Predictive Value (PPV), Negative Predictive Value(NPV), False Positive Rate(FPR), False Negative Rate(FNR) and False Discovery Rate(FDR) which are depicted in below.

Sensitivity

The relationship between a number of true positives (TP) and the sum of true positives and false negatives (FN) is called sensitivity.

\[
\text{Sensitivity} = \frac{TN}{TN + FP}.
\] (14)

Specificity

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

\[
\text{Specificity} = \frac{TP + FN}{TP + FP + TN + FN}.
\] (15)

Accuracy

Accuracy is calculated using measures of sensitivity and specificity. It is denoted as follows,

\[
\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}.
\] (16)
Positive Predictive Value (PPV)

The fraction of positive consequences of the experiment that are considered positive predictive value:

\[ PPV = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}} \]  

(17)

Negative Predictive Value (NPV)

The fraction of negative consequences of the experiment that are considered negative predictive value:

\[ NPV = \frac{\text{True Negative}}{\text{True Negative} + \text{False Positive}} \]

(18)

False Positive Rate (FPR)

FPR is calculated as the number of incorrect positive predictions divided by the total number of negatives. It can also be calculated as 1 – specificity.

\[ FPR = \frac{\text{False Positive}}{\text{False Positive} + \text{True Negative}} \]

(19)

False Negative Rate (FNR)

FNR is calculated as the number of incorrect negative predictions divided by the total number of negatives.

\[ FNR = \frac{\text{False Negative}}{\text{False Negative} + \text{True Positive}} \]

(20)

False Discovery Rate (FDR)

The FDR is the rate that features called significant are truly empty which is defined as.

\[ FDR = \frac{\text{False Positive}}{\text{False Positive} + \text{True Positive}} \]

(21)

4.2. Performance evaluation

The basic idea of proposed methodology is prediction of forged part of the input digital images using multiple stages. The performance is evaluated using different measures. In this work two important stages are available namely, segmentation and classification.
In this section, the performance of both proposed MKFCM and existing K-means and FCM methods are analysed. Identifying forged part of the image is presented by integrating the Deep Learning algorithm using MKFCM method for developing an efficient forged detector of the digital images. Some of the analyzed input database digital images are depicted in the below figure:

Figure 3: **Segmentation Results**

Table 1 shows comparison of original digital image, copied image and its segmented portion. By the proposed methodology, the copied and segmented images are taken for the original digital image. Hence, to analyze the forged part of the digital image.
## Table 2: Evaluation metrics for Sensitivity, Specificity and Accuracy

<table>
<thead>
<tr>
<th>Image Name</th>
<th></th>
<th>Sensitivity</th>
<th></th>
<th>Specificity</th>
<th></th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1</td>
<td>0.99656</td>
<td>0.94126</td>
<td>0.9312</td>
<td>0.99601</td>
<td>0.98961</td>
<td>0.9796</td>
</tr>
<tr>
<td>Image 2</td>
<td>0.98526</td>
<td>0.89284</td>
<td>0.8828</td>
<td>0.99975</td>
<td>0.98453</td>
<td>0.9857</td>
</tr>
<tr>
<td>Image 3</td>
<td>0.97896</td>
<td>0.83190</td>
<td>0.7319</td>
<td>0.99647</td>
<td>0.97986</td>
<td>0.9798</td>
</tr>
<tr>
<td>Image 4</td>
<td>0.97921</td>
<td>0.93150</td>
<td>0.8815</td>
<td>0.99852</td>
<td>0.97980</td>
<td>0.9698</td>
</tr>
<tr>
<td>Image 5</td>
<td>0.97127</td>
<td>0.87577</td>
<td>0.7757</td>
<td>0.99836</td>
<td>0.97984</td>
<td>0.9798</td>
</tr>
</tbody>
</table>

## Table 3: Evaluation metrics for PPV, NPV and FPR

<table>
<thead>
<tr>
<th>Image Name</th>
<th></th>
<th>PPV</th>
<th></th>
<th>NPV</th>
<th></th>
<th>FPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1</td>
<td>0.94688</td>
<td>0.9941</td>
<td>0.994</td>
<td>0.99975</td>
<td>0.9951</td>
<td>0.995</td>
</tr>
<tr>
<td>Image 2</td>
<td>0.99717</td>
<td>1.0000</td>
<td>1.000</td>
<td>0.99869</td>
<td>0.9896</td>
<td>0.989</td>
</tr>
<tr>
<td>Image 3</td>
<td>0.91251</td>
<td>0.9948</td>
<td>0.994</td>
<td>0.99921</td>
<td>0.9900</td>
<td>0.990</td>
</tr>
<tr>
<td>Image 4</td>
<td>0.83069</td>
<td>0.9702</td>
<td>0.970</td>
<td>0.99985</td>
<td>0.9991</td>
<td>0.999</td>
</tr>
<tr>
<td>Image 5</td>
<td>0.93675</td>
<td>0.9920</td>
<td>0.992</td>
<td>0.99928</td>
<td>0.9944</td>
<td>0.994</td>
</tr>
</tbody>
</table>
Table 4: Evaluation metrics for FNR and FDR

Table 2, 3 and 4 shows the performance metrics for both the proposed and existing methodology. Here, measures like sensitivity, specificity, accuracy, PPV, NPV, FPR, FNR and FDR are taken. For analysis, 5 set of digital images are taken. For those input images, its forged part and segmented part were analyzed by clustering and extracting the features for original image. By the performance of MKFCM and existing K-Means and FCM for image 1 the obtained sensitivity measure is 0.99656, 0.9312 and 0.94126 respectively. Likewise, for specificity, the proposed technique achieved is 0.99601 and the accuracy is 0.98605. Hence from the calculation of all measures, it is clear that the proposed MKFCM technique is better than the existing K-means and FCM method. The graph shown below shows the detailed pictorial representation of proposed and existing techniques.
Figure 4: Sensitivity measure of proposed and existing method

Figure 5: Comparison of FCM and K-means method for Specificity metric

Figure 6: Accuracy calculation of proposed and existing methods
While analyzing Figure 4 to 6, the proposed approach achieves the effective result. Hence, the proposed method outperforms better than the existing methods.

For forgery detection, in this work deep learning neural network is utilized. The experimental results obtained from the DNN based forgery detection classification is given in this section. To prove the effectiveness of the algorithm, proposed DNN based classification is compared with different algorithm namely, k-nearest neighbor classifier, random forest and artificial neural network. The performance are analyzed in terms of different metrics namely, sensitivity, specificity, accuracy, PPV, NPV, FPR and FNR.

<table>
<thead>
<tr>
<th>Methods</th>
<th>Accuracy</th>
<th>sensitivity</th>
<th>Specificity</th>
<th>PPV</th>
<th>NPV</th>
<th>FPR</th>
<th>FNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNN</td>
<td>0.93</td>
<td>0.94</td>
<td>0.94</td>
<td>0.972973</td>
<td>0.692308</td>
<td>0.1</td>
<td>0.1</td>
</tr>
<tr>
<td>KNN</td>
<td>0.725</td>
<td>0.4</td>
<td>0.66</td>
<td>0.828571</td>
<td>0.266667</td>
<td>0.6</td>
<td>0.275</td>
</tr>
<tr>
<td>RF</td>
<td>0.675</td>
<td>0.4</td>
<td>0.62</td>
<td>0.818182</td>
<td>0.235294</td>
<td>0.6</td>
<td>0.325</td>
</tr>
<tr>
<td>ANN</td>
<td>0.675</td>
<td>0.5</td>
<td>0.64</td>
<td>0.84375</td>
<td>0.277778</td>
<td>0.5</td>
<td>0.325</td>
</tr>
</tbody>
</table>

**Table 5: Performance based on the classification stage**

The experimental result obtained from classification stage is given in table 5. When analyzing table 5, the proposed DNN based forgery detection approach attain the maximum accuracy of 93% which is 28.23 % better than KNN based forgery detection, 37.7% better than RF based forgery detection and 37.7% better than ANN based forgery detection. This because, DNN has overcome the difficulties present in the other algorithms. Similarly, the maximum sensitivity and specificity is obtained. Also, in this table, the PPV, NPV, FPR and FNR are also discussed. Compared to other method results, proposed method attains the maximum results.
4.3 Comparative analysis

To ensure the effectiveness of the proposed method, a comparison of the proposed process with the work already published is required. Analysis, using the four existing functions. In Amerini et al [18], it is proposed to acquire the local copy and the transcript by making strong links with J-Linkage. In Cozzolino et al. [19], presented comparative results to support the acquisition of copyright. This works based on block-based features. Cozzolino et al. [20], introduced Circular Harmonic Transformations (CHT) and PatchMatch Lying. Similarly, in Xiang et al. [21] Recommended availability of duplicate copies of color images. The methods work fine. Or it should increase the effect. That is why this project proposes to collect DNN to detect crimes. The efficacy of the proposed method was evaluated on the F scale.

![Graphs showing comparative analysis](image)
The complexity of the proposed method in relation to standard treatment F is given in Figure 7. As reported in Figure 7, the proposed CMFD method always exceeds all comparative indicators, with the most significant performance benefit. He is in good condition and has been attacked several times.

5. Conclusion

In this document, the enhanced forgery detection method is proposed with CMFD process using FCM based Deep Learning algorithm. The input digital images are fed into the preprocessing stage using Gaussian filter through which RGB color images are converted into grey scale images. Next to preprocessing, Fuzzy C-means clustering method was applied to divide the preprocessed images to several clusters. Then its unique features are extracted by means of SIFT algorithm. At last, DNN was applied for predicting forged part of the image. The proposed copy move forgery detection method is implemented in the working platform of MATLAB. Also, calculated using various presentation metrics such as sensitivity, clarity, clarity; Positive Predictive Value (PPV), Negative Predictive Value (NPV), False Positive Rate (FPR), False Negative Rate (FNR) and False Discovery Rate (FDR). It is clear that the expected route is better.
than the current one. In the future, an algorithm will be developed to improve the performance of the proposed method.

**Funding:**

There is no funding from any Research or Funding Agency

**Declaration of Interest**

The authors declare that we have no conflict of interest.

**Conflict of Interest:**

The authors declare that we have no conflict of interest.

**Author contribution:**

I have no author contribution.

**References**


