Semiconductor Optoelectronics
ISSN:
1001-5868

ANALYSIS OF COPY MOVE FORGERY DETECTION PROCESS USING FUZZY C MEANS BASED DEEPLEARNING ALGORITHM IN DIGITAL IMAGE

Parameswaran Nampoothiri V
Research Scholar, Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Kanyakumari, Tamilnadu, India
Scientist E, CDAC, Thiruvananthapuram
vpnampoothiri@gmail.com

Dr. N Sugitha
Associate Professor, Department of Electronics and Communication Engineering, Saveetha College of Engineering, Thandalam, Chennai, Tamilnadu, India
sugithavinukumar@gmail.com

Abstract

The popularity of digital photos has developed as a result of technological advancements in the digital environment. Picture alteration has become much easier thanks to powerful and user-friendly photo editing software programmes. Therefore, there was a prerequisite to detect the forged part of the image in efficient manner. Hence, this work emphases on passive forgery recognition on pictures tampered by employing 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 the similar picture on it. Initially, the input digital images are preprocessed through Gaussian filter that was employed to blur the picture to decrease noise. After preprocessing, Multi-kernel Fuzzy C-means clustering (MKFCM) was performed to divide the pictures to numerous clusters then based on unique characteristics the features are extracted by SIFT algorithm. Lastly, with the aid of Deep Learning technique the forged part of the pictures were detected. The experimental analysis demonstrate that the technique was efficient and powerful to identify the forged part of the digital picture and its performance of the proposed strategy was established on numerous forged pictures.

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

1. Introduction

In any area that uses digital photographs, image security is a major concern. 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] is the process of making forged pictures through modifying the real picture content. Digital forensic approaches secure and safeguard multimedia data in instances 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 simply based 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 the utmost frequent kinds of 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. The embedding of a replica is one of the most prevalent methods of picture counterfeiting. In those other terms, this is referred to be a copy-move attack. The embedding procedure is divided into three stages: duplicating a fragment, making adjustments to this segment (strength or geometric), and putting a portion to the region of the screen whose information were intended to be concealed away the end user [10]. One of the images 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 component of a picture onto another section of the same picture. By replicating specific sections, the copy-move fraud seeks to conceal items or overemphasize an idea. 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), to locate certain area(s) of an image that are identical to other area(s) of the picture [2]. Copy-move forgery detection (CMFD) systems have been around for decades and study will guide the same process: Pre-processing, wherein the CMFD algorithms convert the query picture to grayscale 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 that employs matching characteristics to find the original, alleged forgery areas, and post-processing, that sieves out contradictory matches/outliers from matching data and further utilizes the residual pixels to find the complete discovered [7].

Block segment and crucial feature-based methods were the 2 primary classes of CMFD [2]. The identifying and choice of higher entropy areas (key points) is required for key point-based approaches [6]. The final kind of CMFs was key point-based approaches, which extract feature points from pictures using MIFT (Mirror reflection Invariant Feature Transform), SIFT (Scale Invariant Feature Transform), and SURF (Speed up Robust Feature) [9]. Smooth pictures were best handled using block-based models. Nevertheless, because the picture was fragmented into several overlapping chunks, the time complexity is significant [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. DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), 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, Fourier-Mellin Transform, and Polar Cosine Transform (PCT) was used to increase the efficiency of copy move forgery detection approach or geometric distortions [8].

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

2. Related Study

Lot of researchers is analyzed proposed forgery detection methodology. Amongst few of the 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 any prior knowledge of the image or the editing operations performed on it. On the basis of numerous performance measures, a comparison was made between the approach and other tampering detection methods. The approach proved quite 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 local extreme a point. DoG was chosen as a clad approximation for the Laplacian of Gaussian (LoG) and since it was easier to calculate. The Multi-support Region Order-based Gradient Histogram (MROGH) parameter was used to generate descriptive features and thereby increase matching efficiency. They evaluated the theory's resilience to state-of-the-art procedures.

Thirunavukkarasu et al. [13] established a strong process for detecting picture manipulation utilizing Discrete Stationary Wavelet Transform (DSWT) and Multi Dimension Scaling (MDS). Even though a manipulated picture was indistinct, brightness changed, color lowered, as well as reproduced in various spots, the method reduces computing complexity through decreasing feature size and locates the interfered area more effectively. An overall tamper detection performance was better than 97 percent, by a false positive price lesser 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 use the SWT, that what, 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 adapt 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 is both fast and effective. The modified picture was then separated to overlying fixed-size blocks, by each block receiving the Gabor filter. As a result, each block is represented by a Gabor magnitude image. Second, from a histogram of oriented Gabor magnitude (HOGM) of neighboring pixels, statistical characteristics were extracted 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 similarity block pairings. A few settings were utilised to remove the incorrectly identical blocks in order to improve the algorithm's robustness. Fadl et al. [17] have also developed an effectual process to improve Block Matching (BM) based CMF prevention. A use of Polar representation to obtain relevant attributes for each block was the work's major contribution. The primary feature was the use of 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 effectiveness was employed for identifying Copy-Move (CM) areas.

Detecting forged images turns out to be more troublesome when the altered parts were exposed to post activities including scaling, rotation, noise or compression. Another difficulty in copy-move forgery recognition is that copied blocks were from similar picture so they possess similar properties, thus makes it difficult to detect. Yet at the same time, there is a great deal of issues aroused in identifying those pictures. Hence, the lack of solutions to the above said difficulties interested to do study in this region.

3. Proposed CMF identification method

Copy- Move image forgery (CMIF) was duplicating the specific area of a picture by pasting it in certain portion of the identical picture. 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. Existing traditional methods have been used recently to recognize the forgery were not strong, because they don't characterize the operational deviations that properly happened in pictures after tampering either through copy-move or splice. Bench marked images which are forged by performing Copy, Move and Delete operations were assumed in the below example figure 1.

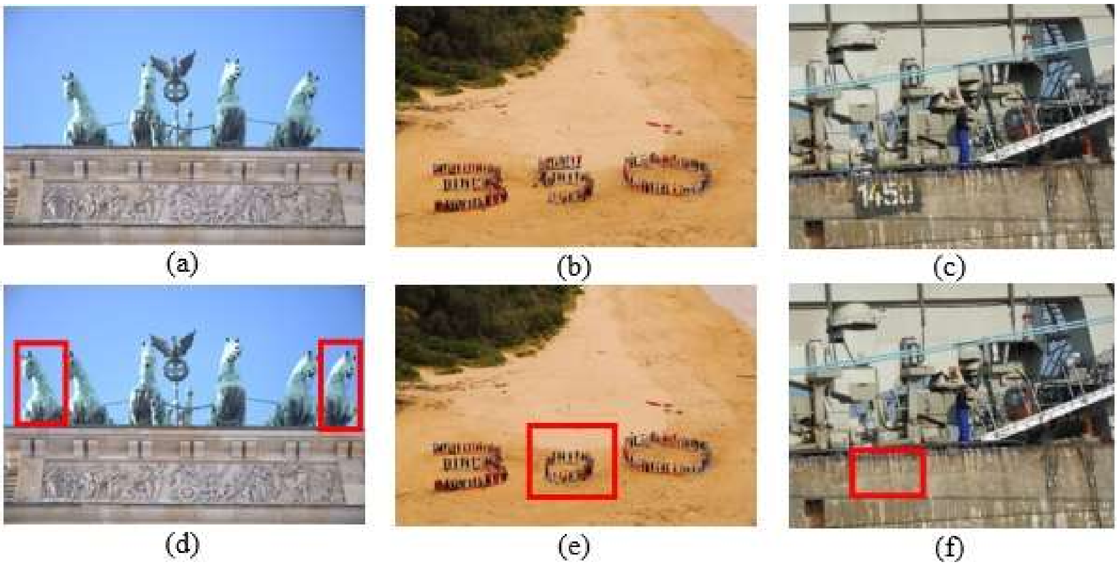


Figure 1: (a) (b) (c) : Real pictures; (d) (e) (f) : Forged Images (Copy, Move and Deleted)

The main objectives of 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 Deep learning algorithm is developed. The projected copy move forgery recognition technique involves three major stages including pre-processing, clustering and DNN based prediction. Initially, during pre-processing, input RGB color picture was changed to gray scale picture and filtered by applying Gaussian filtering. Then the picture was categorized into clusters based on the intensity of pixels using the MKFCM method. After clustering, the clustered images are subjected for feature extraction, where the image's unique characteristic features are extracted by means of SIFT (Scale Invariant Feature Transform). Using the features, the outliers are identified based on matching with the Deep Learning algorithm to exactly predict the forged part of a picture. A schematic illustration of projected CMF recognition method was given in the following figure 2.

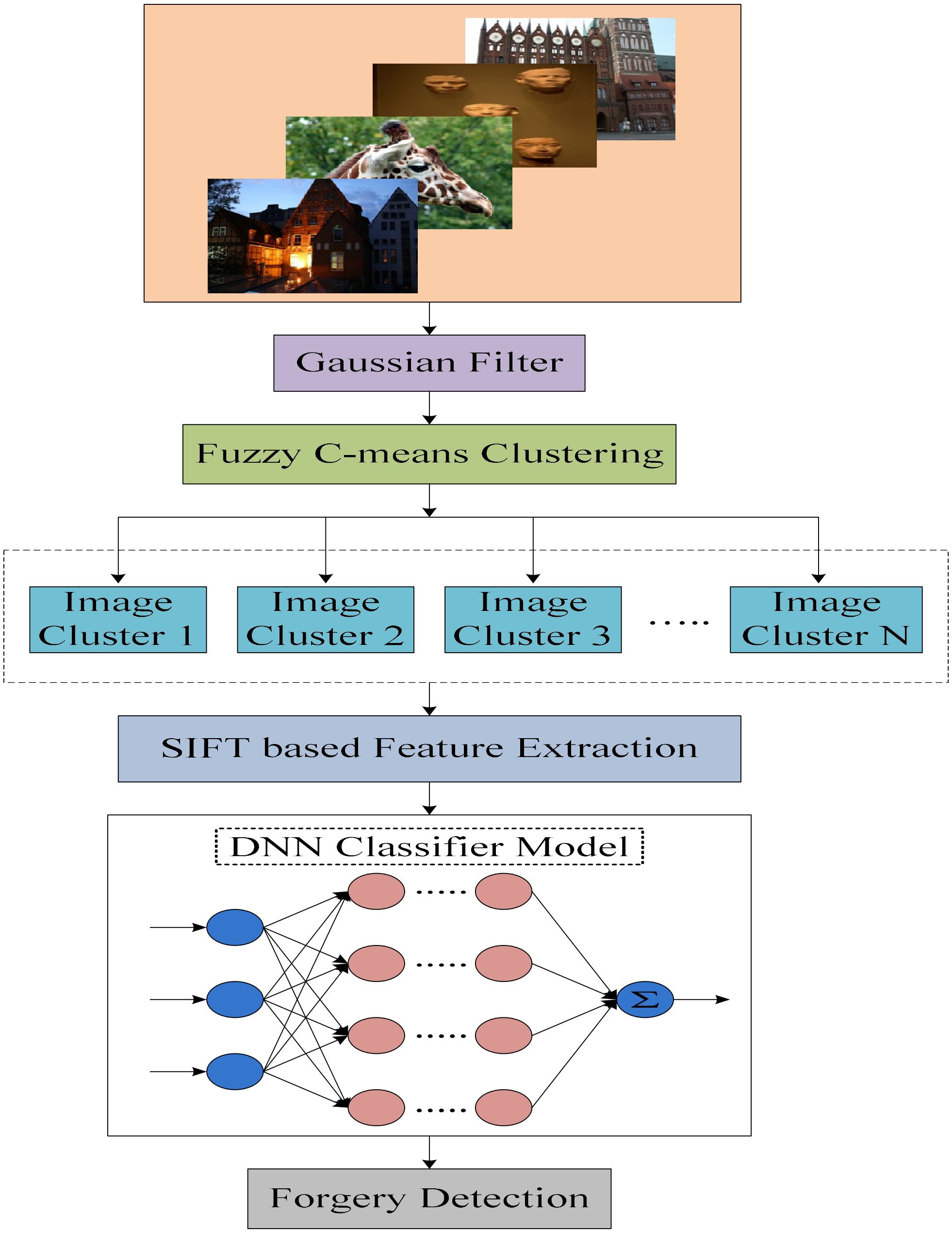


Figure 2: Block illustration for the proposed technique

3.1 Preprocessing:

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

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

The MarrHildreth detectors and the canny detector 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 a variety of other uses, such as picture mosaicking and tone-based plotting of higher energetic ranging pictures.

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

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

Whilst 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 smoothen image f was originate in a frequency area by the given equation

$$F(v,w)=I(v,w)\times J(v,w) \tag{2}$$

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

$$f(y,x)=i(y,x)*j(y,x) \tag{3}$$

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

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 gathering process was employed for find out the location of the forgery detection. Given a number of groups c, MKFCM partitions the data X ={x1,x2,…,xn} to c fuzzy groups through minimalizing the inside cluster sum of squared error. C

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

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,

$V=(v_1,v_2,\ldots,v_c)$ represents a matrix of unidentified cluster centers (prototypes) $v_i\in R^p$, $\|\bullet\|$ characterizes the Euclidean norm

With the intention of abridging Equation (4) the membership function and centroid are employed which are effectively furnished in the following Equations (5) and (6).

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

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

(6)

$$K_H(x_k, c_i) = K_1(x_k, c_i) + K_2(x_k, c_i) \tag{7}$$

Where;

$K_1(x_j, c_i)$ → Linear kernel

$K_2(x_j, c_i)$ → Quadratic kernel

After MKFCM process, the number of groups is obtained. The grouped outputs were 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. His feature is used for extracting distinguishing invariant features from pictures. It's was using a lot in image matching. The SIFT descriptor finds extreme positions over the entire image space. After feature extraction, $1 \times n$ feature for each clustered image will be attained. Then, the extracted features were provided to the input of DNN.

3.4 Deep neural network (DNN) based forgery detection:

An artificial neural network (ANN) by frequent hidden films of units among the input and output layers are called DNN. When the number of possible specimens during the training phase is large, deep learning approaches are quite successful. Here, the projected image forgery model was demarcated as DNN-based method. During this training of DNN, the weights of a neurons were rested in each cycle until the error amid output and input is not inside threshold. The working method of DNN for predicting the forged portion from the images is categorized into two stages. The 1st phase involves the training method and the second phase was involved in a testing procedure. Here, inputs will be a feature of the cluster groups and the Target is fixed as forged/original class labels. DNN is used to train the system depending on the information and target data. In most cases, the training procedure is iterated until the suggested classifier has been validated with the available data.

Let $[R_m]$ = input where $1 \le m \le M$ and ‘ C ’ = output variable. The generalized study of the NN may be provided as ‘ C ’ for output of the complete network and ‘ C_H ’ for output of hidden layer. As in DNN, there were extreme hidden layers, the separate component inputs were reproduced through weights in a 1st hidden layer. In the concealed layer, the particular first hidden component outputs were increased by some other set of weights, etc.

In its 1st hidden layer, the weighted rates of query were given as summing function by the bias of a neuron (equation (8)):

$$C_{H\_1}(x=1,2..,K)=\left(\sum_{m=1}^{M} w_{xm}R_m\right)+b_x \quad (8)$$

Where, b_x continuous value is bias, w_{xm} = interconnectedness weight among the input and hidden layer by M and K representative 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,

$$F\left(C_{H\_1}(x)\right)=\frac{1}{\left(1+e^{-C_{H\_1}(x)}\right)} \tag{9}$$

Where, $F(\cdot)$ = sigmoid activation function

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

$$C_{H\_y}(p)=\left(\sum_{z=1}^{K} w_{pz}F\left(C_{H\_(y-1)}(z)\right)\right)+b_p \tag{10}$$

Where b_p = bias of p^{th} hidden node, w_{pz} = interconnection weight among $(y-1)^{th}$ 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,

$$F\left(C_{H\_y}(p)\right)=\frac{1}{\left(1+e^{-C_{H\_y}(p)}\right)} \tag{11}$$

At the output layer, an output of y^{th} 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

$$C(q)=F\left(\sum_{p=1}^{K} w_{qp}\, f\left(C_{H\_y}(p)\right)+b_q\right) \tag{12}$$

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

Then, 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 (13)

$$\varepsilon=\frac{1}{M}\sum_{m=1}^{M}\left(Actual(C_m)-\Pr edicted(C_m)\right)^2 \tag{13}$$

Where, $\Pr edicted(C_m)$ signifies projected network output and $Actual(C_m)$ = actual output. To achieve a best network structure, the error should be kept to a minimum. As a result, the weight values should be tweaked until the error is reduced at each cycle.

4. Result and discussion

In our study, bench marked pictures were taken for analyses. Initially, preprocessing is applied by means of Gaussian filter where color image is converted into grey scale image. Then Fuzzy C-means clustering method is performed to divide preprocessed image into clusters based on the intensity values. And then its features were extracted with the aid of SIFT algorithm to extract the unique features. Finally, using the Deep Neural Network, forged part of the images was predicted. Mat lab 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.

Sensitivity

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

$$Sensitivity = \frac{No.of\,(TP)}{No.of\,(TP) + No.of\,(FN)} \times 100 \tag{14}$$

Specificity

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

$$Specificity = \frac{No.of\,(TN)}{No.of\,(TN) + No.of\,(FP)} \times 100 \tag{15}$$

Accuracy

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

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \tag{16}$$

PPV

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

$$PPV = \frac{TP}{TP + FP} \tag{17}$$

NPV

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

$$NPV = \frac{TN}{TN + FN} \tag{18}$$

FPR

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

$$FPR = \frac{FP}{FP + TN} \qquad (19)$$

FNR

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

$$FNR = \frac{FN}{FN + TP} \qquad (20)$$

FDR

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

$$FDR = \frac{FP}{FP + TP} \qquad (21)$$

4.2. Performance evaluation:

The basic concept of proposed procedure was prediction of forged part of the input digital pictures by employing multiple phases. The performance was estimated utilizing diverse measures. In this work two important stages are available namely, segmentation and classification.

In this sector, the performance of both projected 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:

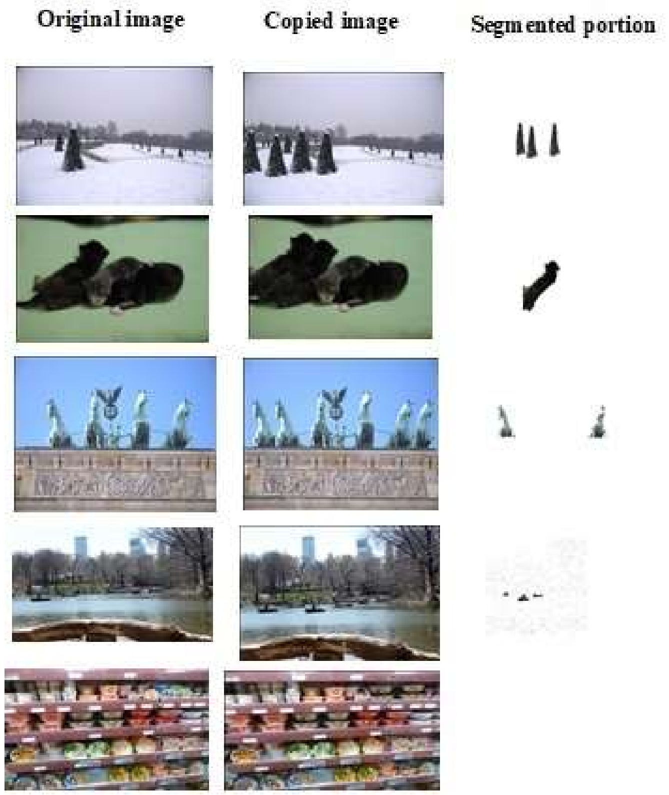


Figure 3: **Segmentation Results**

Table 1 shows comparison of original digital image, copied image and its segmented portion. Bythe proposed methodology, the copied and segmented images were taken for the original digital picture. Hence, to analyze the forged part of the digital image.

Image Name	***Sensitivity***			***Specificity***			***Accuracy***		
	MKFCM	FCM	K-Means	MKFCM	FCM	K-Means	MKFCM	FCM	K-Means
Image 1	**0.99656**	0.94126	0.9312	**0.99601**	0.98961	0.9796	**0.98605**	0.97506	0.96506
Image 2	**0.98526**	0.89284	0.8828	**0.99975**	0.98453	0.9857	**0.98857**	0.97042	0.96042
Image 3	**0.97896**	0.83190	0.7319	**0.99647**	0.97986	0.9798	**0.98583**	0.97014	0.96014
Image 4	**0.97921**	0.93150	0.8815	**0.99852**	0.97980	0.9698	**0.98838**	0.97893	0.96893
Image 5	**0.97127**	0.87577	0.7757	**0.99836**	0.97984	0.9798	**0.98770**	0.97437	0.96437

Table 2: Evaluation metrics for Sensitivity, Specificity and Accuracy

Image Name	***PPV***			***NPV***			***FPR***		
	MKFCM	FCM	K-Means	MKFCM	FCM	K-Means	MKFCM	FCM	K-Means
Image 1	0.94688	**0.9941**	0.994	**0.99975**	0.9951	0.995	**0.00399**	0.0003	0.0003
Image 2	0.99717	**1.0000**	1.000	**0.99869**	0.9896	0.989	0.00025	**0.0000**	0.0000
Image 3	0.91251	**0.9948**	0.994	**0.99921**	0.9900	0.990	0.00353	**0.0001**	0.0001
Image 4	0.83069	**0.9702**	0.970	**0.99985**	0.9991	0.999	0.00148	**0.0002**	0.0002
Image 5	0.93675	**0.9920**	0.992	**0.99928**	0.9944	0.994	0.00164	**0.0001**	0.0001

Table 3: Evaluation metrics for PPV, NPV and FPR

Image Name	***FNR***			***FDR***		
	MKFCM	FCM	K-Means	MKFCM	FCM	K-Means
Image 1	**0.00344**	0.0687	0.068	**0.05312**	0.0058	0.005
Image 2	**0.01474**	0.1171	0.117	**0.00283**	0.0000	0.000
Image 3	**0.02104**	0.2681	0.268	**0.08749**	0.0051	0.005
Image 4	**0.02079**	0.1185	0.118	**0.16931**	0.0297	0.029
Image 5	**0.02873**	0.2242	0.224	**0.06325**	0.0079	0.007

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 namely, PPV, FNR, sensitivity, accuracy, NPV, specificity, FPR and FDR were engaged. 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 was clear that the projected MKFCM technique is improved than the prevailing K-means and FCM method. The graph shown below shows the detailed pictorial representation of proposed and existing techniques.

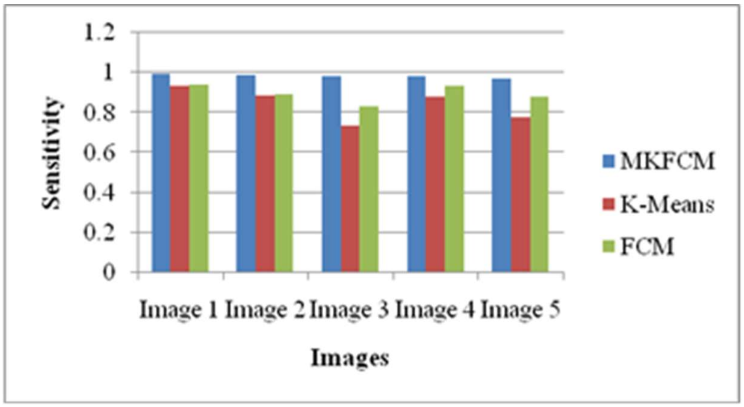


Figure 4: Sensitivity measure of proposed and existing method

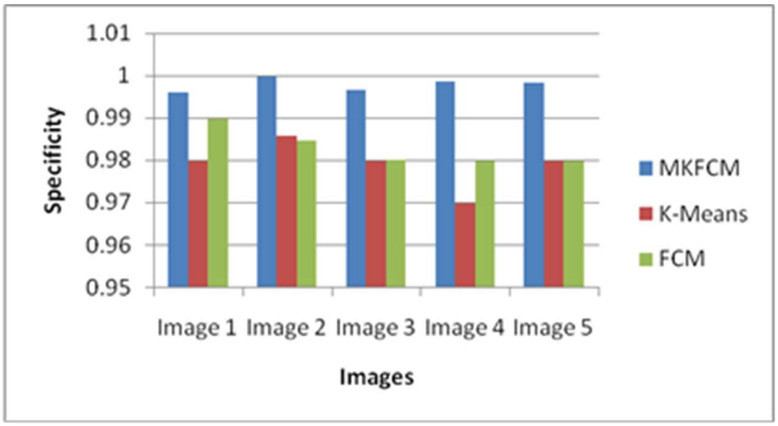


Figure 5: Comparison of FCM and K-means method for Specificity metric

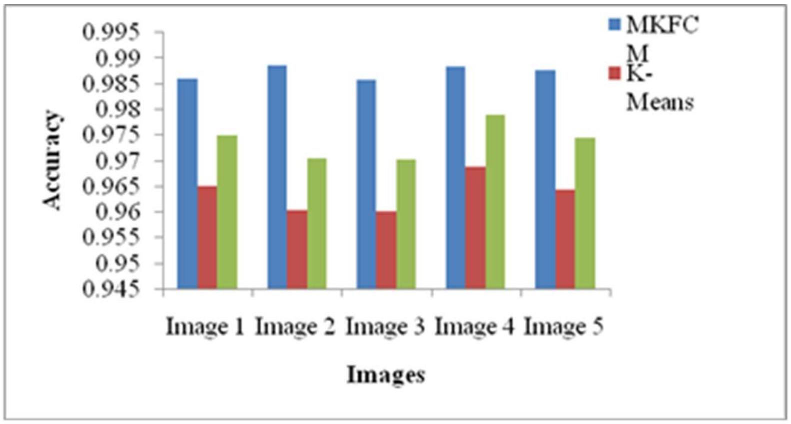


Figure 6: Accuracy calculation of proposed and existing methods

While analyzing Figure 4 to 6, the proposed approach achieves the effective result. Hence, the proposed method outperforms good than the available 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 segment.

To prove the efficacy of the algorithm, projected DNN based classification was compared with different algorithm namely, k-nearest neighbor classifier, random forest and artificial neural network. The performances are analyzed in terms of diverse metrices i.e., FPR, sensitivity, NPV, accuracy, PPV, specificity and FNR.

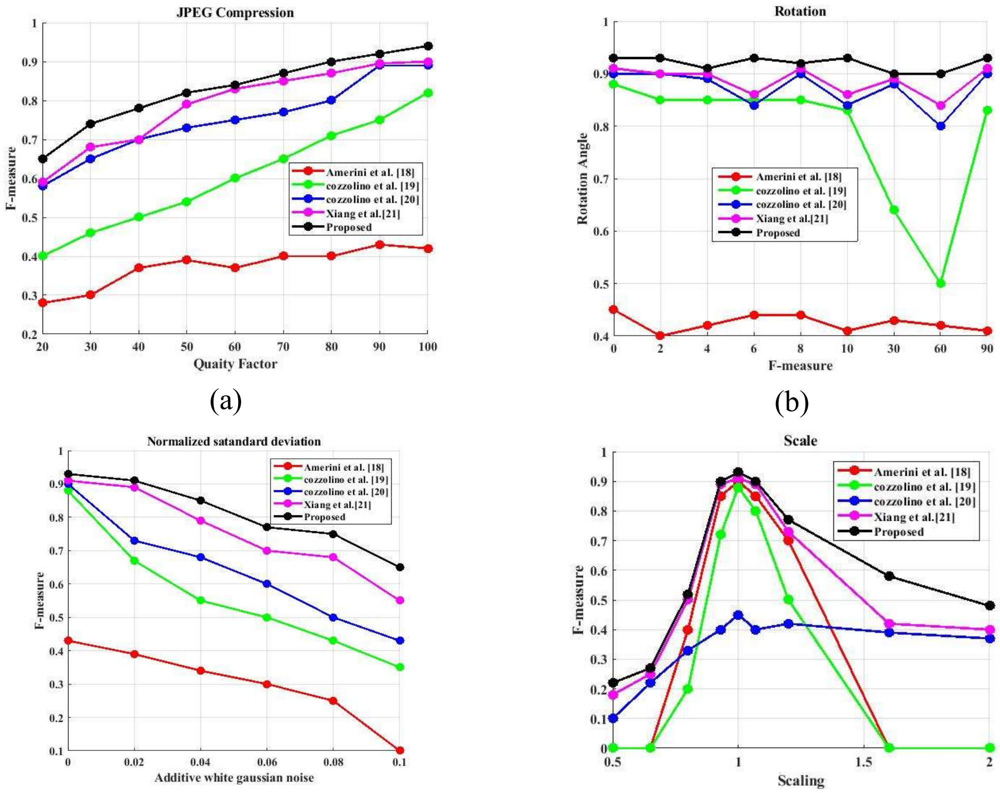
Methods	*accuracy*	*sensitivity*	*specificity*	*PPV*	*NPV*	*FPR*	*FNR*
DNN	**0.93**	**0.94**	**0.94**	**0.972973**	**0.692308**	**0.1**	**0.1**
KNN	0.725	0.4	0.66	0.828571	0.266667	0.6	0.275
RF	0.675	0.4	0.62	0.818182	0.235294	0.6	0.325
ANN	0.675	0.5	0.64	0.84375	0.277778	0.5	0.325

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 method achieve the maximum precision of 93% that was 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 were also discussed. Compared to other method results, projected technique achieves the maximum outcomes.

4.3 Relative study

To verify the efficiency of the proposed procedure, the comparison with the projected methodology with already published work is necessory. For analysis, four existing works are utilized. In Amerini et al [18], CMF identification and localization with regards to 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], Circular Harmonic Transforms (CHT), and PatchMatch based forgery detection is introduced. Similarly, in Xiang et al. [21] key-point-based CMFD for color picture was anticipated. Methods are given the 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 in relative to F-measure.



(a)

(b)

©

(d)

Figure7: F-measure curves for different CMFD methods (a) JPEG compression, (b) Additive white Gaussian noise, (c) Rotation, (d) Scaling

Figure 7 exemplifies the resilience of proposed technique in regard to F-measure cure. The suggested CMFD technique performs better all comparison references, as shown in Figure 7, with a performance benefit that is becoming quite considerable in the ideal situation and under varied assaults.

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 gathering method was executed 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 picture. The projected copy move forgery identification method was implemented in the working platform of MATLAB. It is also calculated using a variety of presenting metrics like sensitivity, PPV, specificity, NPV as well as the FPR, FNR and FDR. It was observed that the anticipated technique outperforms improved than the existing approaches. In future, optimization algorithm to enhance the performance of proposed methodology will be introduced.

References

[1] Wenchang, S., Fei, Z., Bo, Q., & Bin, L. (2016). Improving image copy-move forgery detection with particle swarm optimization techniques. China Communications, 13(1), 139-149.

[2] Soni, B., Das, P. K., & Thounaojam, D. M. (2018). CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection. IET Image Processing, 12(2), 167-178.

[3] Dixit, R., & Naskar, R. (2017). Review, analysis and parameterisation of techniques for copy–move forgery detection in digital images. IET Image Processing, 11(9), 746-759.

[4] Ferreira, A., Felipussi, S. C., Alfaro, C., Fonseca, P., Vargas-Munoz, J. E., Dos Santos, J. A., & Rocha, A. (2016). Behavior knowledge space-based fusion for copy–move forgery detection. IEEE Transactions on Image Processing, 25(10), 4729-4742.

[5] Zandi, M., Mahmoudi-Aznaveh, A., & Talebpour, A. (2016). Iterative copy-move forgery detection based on a new interest point detector. IEEE Transactions on Information Forensics and Security, 11(11), 2499-2512.

[6] Wo, Y., Yang, K., Han, G., Chen, H., & Wu, W. (2017). Copy–move forgery detection based on multi-radius PCET. IET Image Processing, 11(2), 99-108.

[7] Bi, X., & Pun, C. M. (2018). Fast copy-move forgery detection using local bidirectional coherency error refinement. Pattern Recognition, 81, 161-175.

[8] Bi, X., & Pun, C. M. (2017). Fast reflective offset-guided searching method for copy-move forgery detection. Information Sciences, 418, 531-545.

[9] Chauhan, D., Kasat, D., Jain, S., & Thakare, V. (2016). Survey on keypoint based copy-move forgery detection methods on image. Procedia Computer Science, 85, 206-212.

[10] Kuznetsov, A., & Myasnikov, V. (2017). A new copy-move forgery detection algorithm using image preprocessing procedure. Procedia engineering, 201, 436-444.

[11] Mursi, M. F. M., Salama, M. M., & Habeb, M. H. (2017). An improved SIFT-PCA-based copy-move image forgery detection method. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), 6(3), 23-28.

[12] Emam, M., Han, Q., Li, Q., & Zhang, H. (2017, July). A robust detection algorithm for image Copy-Move forgery in smooth regions. In 2017 International Conference on Circuits, System and Simulation (ICCSS) (pp. 119-123). IEEE.

[13] Thirunavukkarasu, V., Kumar, J. S., Chae, G. S., & Kishorkumar, J. (2018). Non-intrusive forensic detection method using DSWT with reduced feature set for copy-move image tampering. Wireless Personal Communications, 98(4), 3039-3057.

[14] Dixit, R., Naskar, R., & Mishra, S. (2017). Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD. IET Image Processing, 11(5), 301-309.

[15] Li, H., Luo, W., Qiu, X., & Huang, J. (2017). Image forgery localization via integrating tampering possibility maps. IEEE Transactions on Information Forensics and Security, 12(5), 1240-1252.

[16] Lee, J. C. (2015). Copy-move image forgery detection based on Gabor magnitude. Journal of Visual Communication and Image Representation, 31, 320-334.

[17] Fadl, S. M., & Semary, N. A. (2017). Robust copy–move forgery revealing in digital images using polar coordinate system. Neurocomputing, 265, 57-65.

[18] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L., & Serra, G. (2013). Copy-move forgery detection and localization by means of robust clustering with J-Linkage. Signal Processing: Image Communication, 28(6), 659-669.

[19] Cozzolino, D., Poggi, G., & Verdoliva, L. (2014, October). Copy-move forgery detection based on patchmatch. In 2014 IEEE international conference on image processing (ICIP) (pp. 5312-5316). IEEE.

[20] Cozzolino, D., Poggi, G., & Verdoliva, L. (2015). Efficient dense-field copy–move forgery detection. IEEE Transactions on Information Forensics and Security, 10(11), 2284-2297.

[21] Wang, X. Y., Li, S., Liu, Y. N., Niu, Y., Yang, H. Y., & Zhou, Z. L. (2017). A new keypoint-based copy-move forgery detection for small smooth regions. Multimedia Tools and Applications, 76(22), 23353-23382.