

An Optimized Fuzzy C-Means with Deep Neural Network for Image Copy-Move Forgery Detection

Parameswaran Nampoothiri V¹ and Dr. N. Sugitha²

¹Research Scholar, Department of Computer Applications, Noorul Islam Centre for Higher Education, Kumaracoil, Kanyakumari, Tamilnadu, India, Scientist E, CDAC, Thiruvananthapuram, India, vpnampoothiri@gmail.com

²Associate Professor, Department of Electronics and Communication Engineering, Saveetha Engineering College, Tandalam, Chennai, Tamil Nadu, India, sugithavinukumar@gmail.com

*Correspondence: Dr. N. Sugitha: sugithavinukumar@gmail.com

ABSTRACT- Copy Move Forgery Detection (CMFD) is one of the significant forgery attacks in which a region of the same image is copied and pasted to develop a forged image. Initially, the input digital images are preprocessed. Here the contrast of input image is enhanced. After preprocessing, Optimized Fuzzy C-means (OFCM) clustering is used to group the images into several clusters. Here the traditional FCM centroid selection is optimized by means of Salp Swarm Algorithm (SSA). The main inspiration of SSA is the swarming behavior of salps when navigating and foraging in oceans. Based on that algorithm, optimal centroid is selected for grouping images. Next, the unique features are extracted from each cluster. Due to the robust performance, the existing approach uses the SIFT-based framework for detecting CMFD. However, for some CMFD images, these approaches cannot produce satisfactory detection results. In order to solve this problem, the current method utilizes the stationary wavelet transform (SWT). After extracting the features, the CMFD detection is done by RB (Radial Basis) based neural network. Additionally, it is computed by means of diverse presentation metrics like sensitivity, specificity, accuracy; Positive Predictive Value (PPV), Negative Predictive Value (NPV), False Positive Rate (FPR), False Negative Rate (FNR) and False Discovery Rate (FDR). The proposed copy move forgery detection method is implemented in the working platform of MATLAB.

Keywords: Copy move forgery detection, False discovery rate, Optimized fuzzy C-means, Salp swarm algorithm, Specificity.

ARTICLE INFORMATION

Author(s): Parameswaran Nampoothiri V and Dr. N. Sugitha;

Received: 06/10/2023; **Accepted:** 04/03/24; **Published:** 30/03/2024;

e-ISSN: 2347-470X;

Paper Id: IJEER 231003;

Citation: 10.37391/IJEER.120142

Webpage-link:

<https://ijeer.forexjournal.co.in/archive/volume-12/ijeer-120142.html>

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.



1. INTRODUCTION

Because a picture was valued at 1000 quotes, the World Wide Web (WWW) now has a significant quantity of digital pictures that are employed in the process of communication. Using freely accessible commercial photo editing software, professionals and non-professionals can easily edit any pre-existing photograph [1]. Medical technology, forensic examination, media, advertising, farming, and, most notably, social media websites like Instagram, Facebook, and Twitter employ digital photographs widely. Active methods and passive procedures are the two main kinds of picture forgery detection techniques. Watermarking and unlawful picture copy detection are active approaches that rely on prior knowledge of the original image [2]. In many cases, though, previous knowledge about an image is not accessible. Without the presence of the main image, passive/blind procedures must be utilized to validate the picture's authenticity [13,14]. Watermarking and unlawful picture copy identification are active approaches that

rely on prior knowledge of the actual picture [3]. In many cases, nevertheless, previous knowledge about a picture is not accessible. Delete or hiding a section in a picture, introducing a new entity to the picture, and distorting image data seem to be the most common image-altering actions [4].

This article discusses digital picture forgery detection, a technique being used to determine if an image has been altered. Copy-move forgery (CMF), image merging, image renovation, and many other techniques are just a few examples of how images can be manipulated. For this reason, identifying a fake image seems to be a difficult task. Therefore, there exists a variety of strategies for dealing with and detecting various forms of forgery [5]. Copy-move forgery detection is related to either key frames or blocks. The image is partitioned into rectangular parts in block-based approaches. Important point-based procedures collect feature points from a picture solely in specific locations, with no picture subdivisions [6]. In general, CM, a kind of forgery where a portion of picture was copied and then inserted on to another portion of a similar picture which helps to hide the important or sensitive information. The major purpose of CMF was to hide important or sensitive information from the original image [7]. This is typically made to make an element "fade away" from a picture through layer it by a section taken from another region of the picture. Since the copied region was part with identical picture, color palette, sound elements, dynamic range, as well as other features of the mirrored area would be consistent with the remainder of the picture. As a result, the human eye does have a significantly harder time identifying copy-move frauds [8, 9]. In addition, the

forger may have applied retouching or resampling techniques to the copied region, making it very difficult to spot copy-moved forging. Retouching entails reduces the duplicated area, introducing noise to a copied region, and so on, whereas resampling entails scaling or spinning the picture [3].

In both cases, preparation of the photos is carried out, like grayscale transformation. Block-based approaches image is partitioned into rectangular parts during the feature extraction phase [12]. The main intention is to find a false image or hidden image for an effectual and strong solution for this type of fake picture.

The rest of this work was alienated to the following segments. The second part will quickly review the numerous efforts and strategies that have been already developed to identify digital picture copy-move forgery. The proposed approach will be thoroughly explained in the third part. The suggested technique's findings will be displayed in segment four. Finally, the fifth section shows the paper's summary.

2. PROBLEM STATEMENT

Large amounts of data can be found in digital images. Pictures can give data to the visual system of humans faster than words can. Because of this, digital information is frequently employed in the context of information dissemination [10]. Imagery data is utilized as crucial proof against a variety of crimes and as proof for a variety of purposes. Heavy photo editing tools and software, on the other hand, are commonly and inexpensively available, allowing the visual content to be easily messed with [11]. Digital image forgery refers to the practice of manipulating an image without such original knowledge by adding, subtracting, or repositioning elements, or by erasing them. This sort of change is extremely difficult to track down and identify visually. Contextually, the motivation behind the alteration could be as sinister as concealing evidence or influencing the target's state of mind. Many algorithms and methods are now being designed to certify the authenticity of images to tackle this issue. The majority of these algorithms, nevertheless, have limitations in terms either of computation time or accuracy rate. Furthermore, several of the techniques in the literature are limited to simple copy-move forging scenarios, whereas others contribute significantly to the detection of complex manipulation. These methods, nevertheless, are not without flaws [8,9]. This lack of a solution to the problem motivated me to do research in this field by proposing a new detection system.

3. PROPOSED METHODOLOGY

Copying and pasting material in the same image creates a copy-move fake. Identifying copied picture portions, even whether they are somewhat diverse from one other, was the determination of copy-move forgery identification which help to determine whether an image is pristine or forged. Firstly, the input pictures were assumed to be the pre-processing phase where histogram equalization was executed to improve the difference of input pictures. After subjecting the images to pre-processing, clustering was accomplished to group the pixels

based on similarity with an aid of the Optimized Fuzzy C-means algorithm.

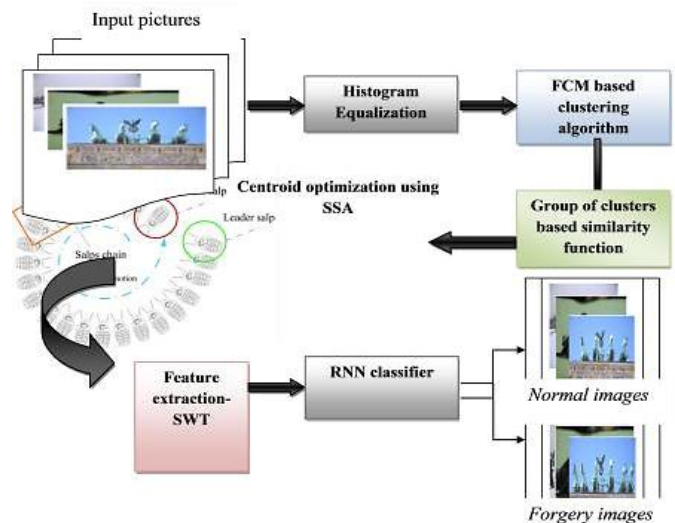


Figure 1: Overall Proposed Architecture

The further centroid of the FCM is optimally selected by using Slap Swarm Algorithm. Then the characteristics were take-out utilizing SWT. Then, the RBNN classifier was utilized to train the images based on extracted features. Based on the process of RBFNN, the forgery and non-forgery images are classified. During the training time itself, the forged and non-forged pictures are classified. When the new image is given for testing, it will analyze the input image as forged and non-forged pictures based on the trained data. The entire architecture of the proposed technique for CMF identification is given in figure 1.

The proposed work is classified into the following stages,

- ✓ Pre-Processing using Histogram equalization
- ✓ Clustering based on Optimized Fuzzy C-means
- ✓ Centroid selection is optimized by SSA
- ✓ Extracting the feature using SWT to generate decomposed approximate image
- ✓ Detection of forged image by means of RBNN

3.1 Pre-Processing

To execute the proposed CMFD method, at the beginning, pre-processing was utilized to diminish the redundant noise components for enhancing the contrast of image. The pre-processing technique was carried out with the help of Histogram Equalization, where the disparity of the picture was augmented. The detailed view of Histogram equalization and its working principal is given as follows:

3.2 Histogram equalization

The Histogram equalization method aids in improving picture quality in this section. In terms of achieving stronger contrast, the histogram equalization technique spreads the intensity values across the entire range of outcomes. This strategy is extremely beneficial when a picture has a high contrast value, including when the backdrop and forefront are both luminous around the same period, or when both of these are gloomy at the same period.

Histogram equalization is the conversion of gray levels ‘ S ’, as gray levels ‘ t ’, where the movement of gray level ‘ t ’ is equal. The approach expands the series of gray values for the histogram maximum in this transformation. The transformation increases the detection rate of several picture features by increasing brightness for the majority of the input image.

The probability density function of a pixel intensity level ‘ Q_m ’, can be provided by *equation (1)*:

$$pdf_q(Q_m) = \frac{P_m}{P} \quad (1)$$

Where, $0 \leq Q_m \leq 1$, $m=0,1,\dots,255$, P_m is the number of pixels at intensity level ‘ Q_m ’, and P denotes the total number of pixels; Then, the histogram might be resulting by plotting $pdf_q(Q_m)$ against Q_m . At this period, a new intensity level r_m is formed as described as *equation (2)*:

$$r_m = \sum_{n=0}^m \frac{P_n}{P} = \sum_{n=0}^m pdf_q(Q_n) \quad (2)$$

As a consequence, the contrast is increased locally, and the brightness of each pixel is adjusted in accordance with its immediate surroundings. When there is a significant variation in intensity among the lowest and highest saturation levels, the image is said to have strong contrast. As a result, by equalizing the image’s Histogram, places with lesser local contrast could receive a greater contrast without hurting the overall contrast. Following image contrast enhancement, the pictures are subjected to a grouping procedure based on the similarity parameters.

3.3 Optimized Fuzzy C-Means Clustering Model

Commonly, c-means were the best known, well improved clustering studies since they are least square models. FCM [14] is chosen for the proposed research because of the following reasons:

- It produces the good outcomes for overlapped data sets and outperforms the k-means method.
- Despite k-means, where a data point can only connect to 1 cluster center, herein each cluster center was allocated association, allowing a data point to belong to several cluster centers.
- As a result, fuzzy c-means is related with c-means clustering techniques; Fuzzy c-means was particularly common because it can deal up overlapping clusters.

In the proposed research, FCM strategy helps to group the image pixel values based on likeness standards. The membership values are assigned to each picture or the center choice is used to cluster them. To achieve this, following equations are processed:

3.3.1 Initialization of FCM

For grouping similar images obtained from pre-processed image, initialize the data points and its centers for all the considered input images in terms of X and C respectively,

shown in *equation (3)* and *eq. (4)*. The objective function of FCM and its center selection process are described in *table 1*.

$$x = \{x_1, x_2, \dots, x_n\} \quad (3)$$

$$c = \{c_1, c_2, \dots, c_n\} \quad (4)$$

Table 1: The objective function of FCM and its center selection

Steps	Equation	Purpose
Objective Function of FCM	$OF = \sum_{i=1}^n \sum_{j=1}^c m_{ij}^a \ x_i - c_j\ ^2$	The major aim of FCM is to minimize objective function by selecting optimal centroid for grouping the images.
The expansion of the above equation is		
Fuzzy membership function	$m_{ij} = \frac{1}{\sum_{k=1}^c (Eu_{ij}/Eu_{ik})^{2/(a-1)}}$	For each initialized parameter, its membership function is calculated.
Fuzzy center c_j	$c_j = \left(\frac{\sum_{i=1}^n (m_{ij})^a x_i}{\sum_{i=1}^n (m_{ij})^a} \right) \quad \forall j = 1, 2, \dots, c$	The optimal c_j is chosen by an optimization algorithm (SSA)

3.3.2 Variable Description

The term objective function is expressed as OF , n is the number of data point, c_j represents the j^{th} cluster center, a is the fuzziness index $a \in [1, \infty]$, c represents the number of cluster center, m_{ij} indicates the fuzzy membership of i^{th} data to j^{th} cluster center, Eu_{ij} belongs the Euclidean distance between i^{th} data and j^{th} cluster center. Similarly; Eu_{ik} indicates the Euclidean distance between i^{th} data as well as k^{th} cluster center”. Where $\|x_i - c_j\|$ represents the Euclidean distance between i^{th} data and j^{th} cluster center; k is the number of iteration steps. Repeat fuzzy membership function m_{ij} and cluster center c_j steps until maximum OF is achieved.

3.3.3 Optimal center selection

To identify the optimal centroid, we have to choose the accurate center point by the use of centroid optimization. The optimal centroid is chosen by the meta-heuristic algorithm called SSA. By executing the number of iterations of SSA, the optimal centroid value is determined. The images with similarity pixels are grouped on the basis of evaluated centroid value.

3.3.4 Centroid Optimization by means of FCM

The optimal cluster center selection gives very accurate classification results, for this centroid optimization is done using SSA algorithm. Here, the center points of FCM i.e. $c_{j=1,2,\dots,n}$ is considered as a number of populations. Its objective function is computed as $OF_{co} = \text{optimal}(\text{centerpoint}())$, where OF_{co} indicates centroid optimization of FCM.

3.4 Salp Swarm Algorithm (SSA)

For optimally selecting the centroid value, SSA based optimization algorithm is utilized. SSA is a novel optimization technique (Mirjalili et al. 2017) [28], which mimics the behavior of Salps in nature; salps are a kind from the Salpidae's family, and they are barrel-shaped planktonic tunicate. SSA starts by dividing the population into two groups namely the leader and the followers. The front salp of the chain is called the leader, and the other salps are called the followers. The salps' position is determined in n -dimensions which represent the search space of a problem and n represents the problem's variables. These salps search for a food source which indicates the target of the swarm. Here the centroid is optimized by means of SSA technique and the position should be updated frequently, so, the following equation (5) is used to perform this action to the salp leader:

$$S_j^1 = \begin{cases} f_j + R_1[(U_j - L_j)R_2 + L_j]R_3 \geq 0 \\ f_j - R_1[(U_j - L_j)R_2 + L_j]R_3 < 0 \end{cases} \quad (5)$$

Where, S_j^1 indicates the position of the first salp (leader) within j^{th} dimension, the position of the food source in j^{th} dimension is indicated as f_j ; the upper bound and lower bound is denoted as U_j and L_j respectively; R_2 , and R_3 are generated randomly in the interval of [0,1] to maintain search space. Likewise, the parameter R_1 is very important coefficient due to its role in the balancing between the exploration phase and the exploitation phase which is calculated as follows in equation (6)

$$R_1 = 2e^{-(4l/l_{max})^2} \quad (6)$$

Where l is the current iteration and l_{max} is the maximum number of iterations. After updating the leader's position, the SSA starts to update the follower's position using the following equation (7)

$$S_j^i = \frac{1}{2}[S_j^i + S_j^{i-1}] \quad (7)$$

S_j^i represents the i^{th} follower position within j^{th} dimension and i is greater than 1. Finally, the optimal centroids are determined based on the optimal position of the salps on account of increasing iterations. Algorithm is outlined as follows in table 2.

Table 2: Pseudo code: SSA

1. Initialize a population j^{th}
2. Repeat
3. Compute the objective function for each solution S_i
4. Update the best salp(solution)
5. Update R_1 using $R_1 = 2e^{-(4l/l_{max})^2}$
6. For $i = 1: N$ do
7. If $i == 1$ then
8. Update the position of salp using

$$S_j^1 = \begin{cases} f_j + R_1[(U_j - L_j)R_2 + L_j]R_3 \geq 0 \\ f_j - R_1[(U_j - L_j)R_2 + L_j]R_3 < 0 \end{cases}$$
9. Else

10. Update the position of salp using $S_j^i = \frac{1}{2}[S_j^i + S_j^{i-1}]$
11. End if
12. End for
13. Until ($l < l_{max}()$)
14. Return the best solution f

3.5 Feature extraction using SWT

Every picture includes information or features that weren't noticeable to the naked eye. We extract this key characteristic using feature selection methods. The proposed method extracts stationary wavelet transform (SWT)-based characteristics for detecting forgeries in digital photographs to reduce the query picture. SWT is performed to each image after the centroid selection phase to yield four frequency sub-bands: LL, HL, LH as well as HH.

A calculation sub-band of the stationary wavelet based employed precisely because it contains the majority of the data that is most suitable for forgery detection. SWT is widely used by its excellent spectrum and spatial localization features.

Generally, in DWT, the query picture was convoluted by the lower $k^{[n]}$ and higher pass $g^{[n]}$ filters and devastate through a factor of 2 to attain the wavelet coefficients. In SWT, on the other hand, an input convolving the picture using lower pass and higher pass filters in a comparable pattern, but no decimation is undertaken to produce the wavelet coefficients [2]. As a result, the SWT at levels for a brightness image of size can be stated in mathematical formulae as follows in equation (8), (9) and eq. (10):

$$LH_{i+1}(N, M) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} k_x^i g_y^i LL_i(N+x, M+y) \quad (8)$$

$$HL_{i+1}(N, M) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} g_x^i k_y^i LL_i(N+x, M+y) \quad (9)$$

$$HH_{i+1}(N, M) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} g_x^i g_y^i LL_i(N+x, M+y) \quad (10)$$

The sub-images LH, HH as well as HL attained by employing above equations which signify the horizontal, vertical as well as diagonal sub bands. Nevertheless, the LL sub band was stated as in equation (11),

$$LL_{i+1}(N, M) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} k_x^i k_y^i LL_i(N+x, M+y) \quad (11)$$

Where $N=1,2,\dots,W$, $M=1,2,\dots,H$, k is a lower passed filter and g is a higher passed filter. An approximation sub-bands (LL)

attained over Y was measured for an assessment of projected forgery recognition method.

1st level disintegration of 2D picture by SWT was displayed in below figure which evidently circumstances that a picture of size $W \times H$ disintegrated to four sub bands: horizontal (LH), approximation (LL), vertical (HL) and diagonal (HH), where all the sub-bands have similar size $W \times H$ like the query picture. Where W, H designates the total number of columns and rows of LL. Finally, from the decomposed input image, the approximate picture was taken as input for the next stage.

3.6 Classification by employing Radial basis Function based neural network

The classifier using the Radial basis Function based neural network (ORBFNN) technique after we select the suitable information of the input dataset. ORBFNN is used in this case to recognize and classify photos as normal or forgery. The following is a complete explanation of the ORBFNN technique. The number of neurons, radii, relative centers, and weight are indeed parameters employed in the RBFNN. Together with aid of Broom head and Lowe, RBFN [2] were included to the NN. On the contrary, traditional study was a system of local units which was intrigued through the existence of various local reaction elements in human brain. Neurons by a finely tuned user can interact can be originate in many portions of nervous system, such as cells in an auditory system that detect minor bands of occurrences/cells in a visual cortex that detect bars moving in the specific way/other aesthetic aspects in a minor area of the pictorial arena. The RBFNN, a type of NN with 3 layers: an input, a hidden and an output layer. To classify a data as normal or fake, the RBFNN is used. The RBFNN receives the image's optimally picked features as input.

The RBF-NN output was designed as per *equation (12)*,

$$O = \sum_{i=1}^N W \zeta_i(f, c_i) = \sum_{i=1}^N W \zeta_i(\|f - c_i\|_2) \quad (12)$$

Where,

$f \in R^{n \times 1}$ represents an input vector

$\zeta_i(\cdot)$ = radial basis function from $R^{n \times 1}$ (set of all +ve real number) to R .

$\|\cdot\|_2$ indicates the Euclidean norm

W = weights of linking that ascribes unseen neuron number i as well as an output neuron number O = output layer

N = sum of neurons in an unseen sheet

$c_i \in R^{n \times 1}$ = RBF centers in an input vector space.

The input layer was ready to receive data. The unseen layer uses a non-linear function to change the data from the input space to the invisible space. The output layer is continuous, and the network's reaction is revenue.

3.1 Experimental Setup

We used MATLAB Version 2014a on a 32-bit Windows 10 machine with 8 GB of RAM to carry out the planned segments

and classification of Normal as well as forgery images. The basic hint of our proposed procedure was to recognize the forgery portion of the input digital picture utilizing numerous phases. The performance was assessed by diverse evaluation metrics. Herein, we have classified the performance degree of both segmentation and classification outcomes. Also, the proposed work was in comparison with prevailing methodologies to display the superiority of the projected method. The research was prepared with a digital image dataset engaged online and their performance actions were estimated. Few of the specimen images gathered from the online taken for the study are given below *figure 2*.

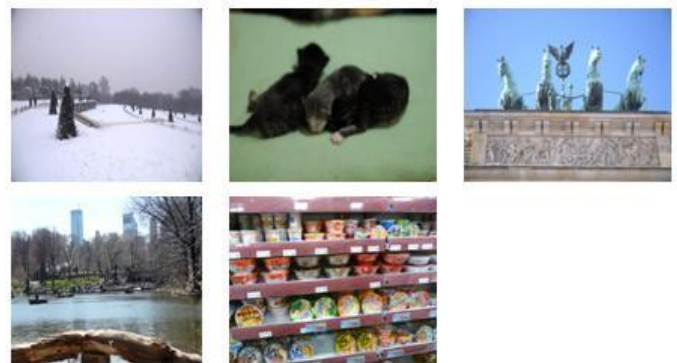


Figure 2: Sample input pictures

These were the freely available database images taken for our research work. Among several online sources, we have considered 5 input images for analysis for forgery detection.

4. RESULTS AND DISCUSSIONS

The performance efficiency of the projected scheme was assessed by computing the measures namely, sensitivity, accuracy, specificity, Positive Predictive Value (PPV), False Positive Rate (FPR), False Negative Rate (FNR), Negative Predictive Value (NPV), as well as False Discovery Rate (FDR) in the process. The metrics are evaluated for the proposed FCM-based SSA technique which was shown below in *table 3*.

Table 3 displays the outcome of performing actions that were achieved in MATLAB execution. The accurateness obtained for all the taken input images is nearer to 1 and it is much more efficient than the existing FCM approach. Also, while referring the *table 4*, all the measures obtained for the proposed work are best than the existing one. The comparison pictorial representation displays that the proposed and existing study are evaluated employing some metrics similar to sensitivity, accuracy, accuracy, NPV, PPV, FNR, and FDR/FPR. For forgery recognition, the input pictures were categorized as normal images and non-forged images by employing the proposed RNN algorithm. Here we compared the proposed FCM-SSA technique with the default FCM algorithm. *Table 2* exemplifies the outcomes of the proposed (RNN) and prevailing classification algorithms. For instance; the accuracy obtained for the proposed work is 0.94 and for other algorithms, it is 0.9 for DNN, 0.66 for KNN, 0.62 for RF, and 0.62 for ANN.

Table 3: Proposed segmentation outcome for different metrics






FCM-SSA								
Image Name	Sensitivity	Specificity	Accuracy	PPV	NPV	FPR	FNR	FDR
	0.998	1.000	1.000	0.982	1.000	0.000	0.002	0.018
	0.917	0.988	0.984	0.850	0.994	0.012	0.083	0.150
	0.921	1.000	0.999	0.960	0.999	0.000	0.079	0.040
	0.986	0.997	0.997	0.925	0.999	0.003	0.014	0.075
	0.962	1.000	1.000	1.000	1.000	0.000	0.038	0.000

Table 4: Classification results for proposed and existing methods

Proposed and Existing	Sensitivity	Specificity	Accuracy	PPV	NPV	FPR	FNR
RNN	0.95	0.9	0.94	0.975	0.819	0.1	0.05
DNN	0.9	0.9	0.9	0.973	0.694	0.1	0.1
KNN	0.735	0.4	0.66	0.829	0.267	0.6	0.275
RF	0.685	0.4	0.62	0.819	0.236	0.6	0.325
ANN	0.685	0.4	0.62	0.819	0.236	0.6	0.325

Also, by the overall analysis, it was clear that the proposed method attains an effective outcome than other classifiers. For comparison; the result determines that the proposed study attains a value between 0.9 and 1. But the existing approach DNN provides the next level resultant in the range from 0.7 to 0.999. Likewise, the results are computed for the existing algorithms namely, KNN, RF, and ANN. These classification techniques obtain the minimum outcome compared with the proposed algorithm, *figure 3*. From the overall study, the proposed technique attains the best performances of other existing methods.

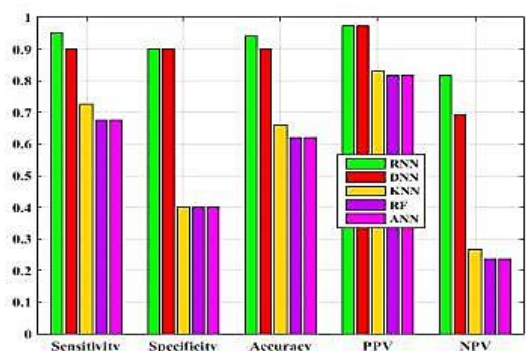


Figure 3: Comparison graph for proposed and existing works using different metrics

5. CONCLUSION

A strong method for CMF recognition and localization in digital pictures was projected. The main goal of our work was to recognize the forgery portion of digital pictures. The feature extraction stage is carried out using the SWT algorithm for extracting the appropriate features. The extracted features were fed into the grouping phase where RBFNN was achieved to categorize normal and forgery imageries. The whole work was applied in the working platform of MATLAB. Diverse evaluation metrics were examined to differentiate between projected and prevailing methodologies. From the overall study, it is clear that our proposed method attains an efficient outcome than other prevailing studies. The authors tested their proposed methodology on different digital image datasets collected from web sources. Thus, the performance of a projected scheme was higher than other tested CMFD techniques. For future work, we will apply the same concept to forged videos.

REFERENCES

- [1] Fadl, S. M., & Semaary, N. A. (2014, December). A proposed accelerated image copy-move forgery detection. In 2014 IEEE Visual Communications and Image Processing Conference (pp. 253-257). IEEE.
- [2] Paul, K. H., Akshatha, K. R., Karunakar, A. K., & Seshadri, S. (2019, April). SURF-Based Copy Move Forgery Detection Using kNN Mapping. In Science and Information Conference (pp. 234-245). Springer, Cham.
- [3] Christlein, V., Riess, C., Jordan, J., Riess, C., & Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on information forensics and security*, 7(6), 1841-1854.
- [4] 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.
- [5] Huang, H. Y., & Ciou, A. J. (2019). Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation. *EURASIP Journal on Image and Video Processing*, 2019(1), 1-16.
- [6] Qayyum, H., Majid, M., Anwar, S. M., & Khan, B. (2017). Facial expression recognition using stationary wavelet transform features. *Mathematical Problems in Engineering*, 2017.
- [7] Wang, C., Zhang, Z., & Zhou, X. (2018). An image copy-move forgery detection scheme based on A-KAZE and SURF features. *Symmetry*, 10(12), 706.
- [8] Yeap, Y. Y., Sheikh, U. U., & Ab Rahman, A. A. H. (2018, March). Image forensic for digital image copy move forgery detection. In 2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA) (pp. 239-244). IEEE.
- [9] Ibrahim, H., & Kong, N. S. P. (2007). Brightness preserving dynamic histogram equalization for image contrast enhancement. *IEEE Transactions on Consumer Electronics*, 53(4), 1752-1758.
- [10] Mirjalili, S., Gandomi, A. H., Mirjalili, S. Z., Saremi, S., Faris, H., & Mirjalili, S. M. (2017). Salp Swarm Algorithm: A bio-inspired optimizer for engineering design problems. *Advances in Engineering Software*, 114, 163-191.
- [11] Shen, W., Guo, X., Wu, C., & Wu, D. (2011). Forecasting stock indices using radial basis function neural networks optimized by artificial fish swarm algorithm. *Knowledge-Based Systems*, 24(3), 378-385.
- [12] Raju, P. M., & Nair, M. S. (2022). Copy-move forgery detection using binary discriminant features. *Journal of King Saud University-Computer and Information Sciences*, 34(2), 165-178.
- [13] Li, Q., Wang, C., Zhou, X., & Qin, Z. (2022). Image copy-move forgery detection and localization based on super-BPD segmentation and DCNN. *Scientific Reports*, 12(1), 1-12.

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



© 2024 by the Parameswaran Nampoothiri V and Dr.N.Sugitha. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).