



## AN OPTIMIZED FUZZY C-MEANS WITH DEEP NEURAL NETWORK FOR IMAGE COPY-MOVE FORGERY DETECTION

Parameswaran Nampoothiri V<sup>1</sup>, Dr. N Sugitha<sup>2\*</sup>

<sup>1</sup>Research Scholar, Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Kanyakumari, Tamilnadu, India

Scientist E, CDAC, Thiruvananthapuram

<sup>2</sup> Professor, Department of Electronics and Communication Engineering, Saveetha College of Engineering, Chennai, Tamil Nadu, India

Email: <sup>1</sup> vpnampothiri@gmail.com, <sup>2</sup>sugithavinukumar@gmail.com

Corresponding Author: sugithavinukumar@gmail.com

**Abstract-** CMFD (Copy Move Forgery Detection), a significant fake attack in a region of the same image was copied and inserted to develop a forged image. Initially, the input digital images are preprocessed. Here the contrast of the input image is enhanced. After preprocessing, Optimized Fuzzy C-means (OFCM) gathering is employed for clustering the pictures for various clusters. Here the traditional FCM centroid selection was enhanced beside Salp Swarm Algorithm (SSA). The major motivation of SSA was the swamped conduct of salps when directing and scavenging in oceans. Based on that algorithm, the 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. To resolve this issue, the current method utilizes the stationary wavelet transform (SWT). After extracting the features, the CMFD detection was executed by RB (Radial Basis) based neural network. Moreover, it was calculated employing various presentation metrics including sensitivity, precision, Predictive Value (PPV), specificity, False Discovery Rate (FDR), False Negative Rate (FNR), Positive False Positive Rate (FPR), and Negative Predictive Value (NPV). The projected CMFD strategy was implemented in the functioning stage of MATLAB.

**Keywords-** Copy Move Forgery Detection; False Discovery Rate; Optimized Fuzzy C-means; Salp Swarm Algorithm, specificity.

### I. 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 2 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 [5,6]. Copy-move forgery detection is related to either keyframes 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 [7]. 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.

## II. 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.

### III. 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. 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.

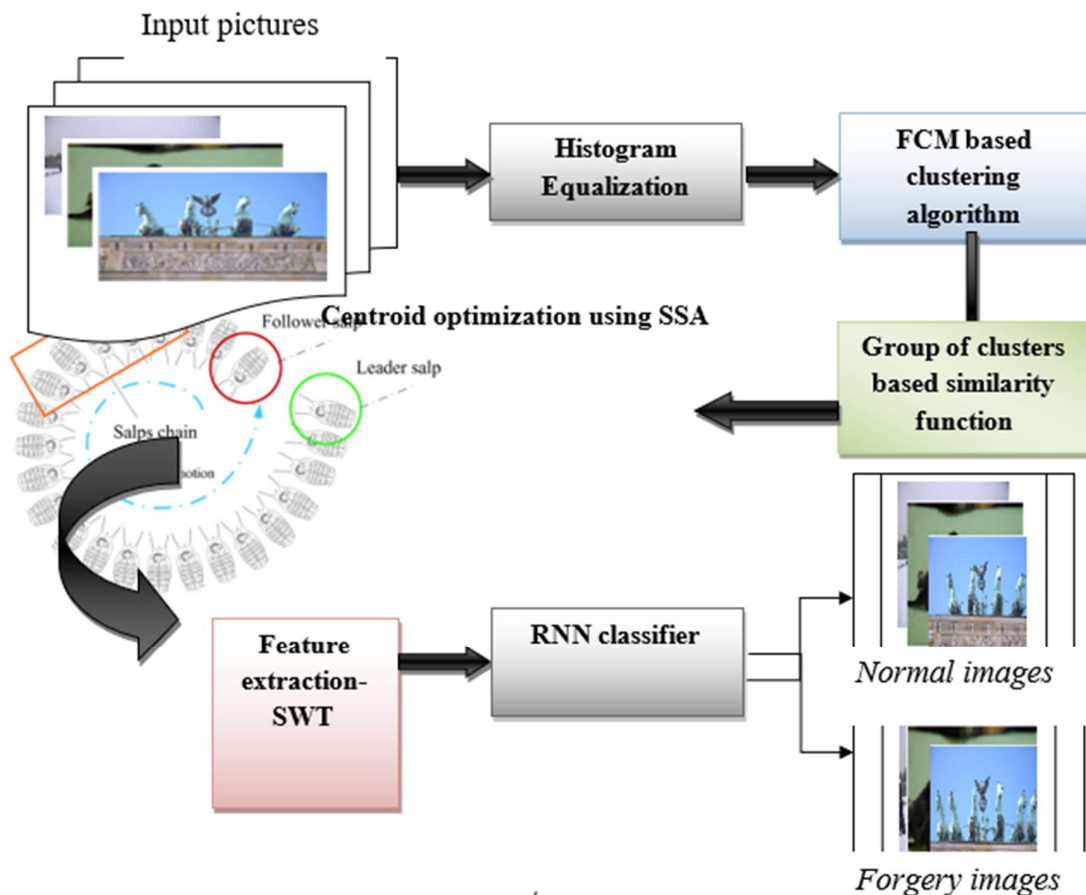


Figure 1: Overall proposed architecture

**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.

**IV. RESULTS AND DISCUSSION**

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 1.

**Table 1: Proposed segmentation outcome for different metrics**

FCM-SSA								
<i>Image Name</i>	<i>sensitivity</i>	<i>specificity</i>	<i>accuracy</i>	<i>PPV</i>	<i>NPV</i>	<i>FPR</i>	<i>FNR</i>	<i>FDR</i>
	0.998	1.000	1.000	0.98 2	1.00 0	0.00 0	0.00 2	0.01 8
	0.917	0.988	0.984	0.85 0	0.99 4	0.01 2	0.08 3	0.15 0
	0.921	1.000	0.999	0.96 0	0.99 9	0.00 0	0.07 9	0.04 0



	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 1 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 2, 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: Classification results for proposed and existing methods**

<b>Proposed and Existing</b>	<b>Sensitivity</b>	<b>Specificity</b>	<b>Accuracy</b>	<b>PPV</b>	<b>NPV</b>	<b>FPR</b>	<b>FNR</b>
RNN	<b>0.95</b>	<b>0.9</b>	<b>0.94</b>	<b>0.975</b>	<b>0.819</b>	<b>0.1</b>	<b>0.05</b>
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

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.

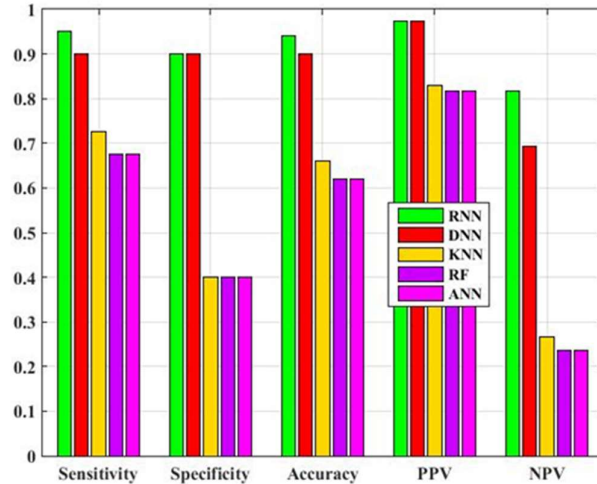


Figure 3: Comparison graph for proposed and existing works using different metrics

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.

## V. 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.

## ACKNOWLEDGEMENT

The authors are thankful to the Department of CDAC for the research support

## REFERENCES

1. Fadl, S. M., & Semary, 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.