International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

IJISAE

ISSN:2147-6799 www.ijisae.org Original Research Paper

Adaptive Threshold-based Reserved G2NN Feature Matching with Hybrid Deep Feature Learning for Copy-Move Image Forgery Detection

Mr. Sai Pratheek Chalamalasetty[1], **Dr. Srinivasa Rao Giduturi***[2]

Submitted:12/03/2024 **Revised**: 27/04/2024 **Accepted**: 04/05/2024

Abstract: Different image editing devices have been utilized for performing image forgery activities on social media in recent days. Then, the copied images are placed in various locations of the image. But, the important disadvantage of using these forgery detection approaches is detecting the tampered regions with less efficiency. The ultimate aim of this scheme is to investigate novel copy-move image forgery identification with the assistance of deep learning and matching procedure. In the first step, the benchmark datasets are gathered from different public sources and perform pre-processing using the Weiner filtering and contrast stretching process. Further, the feature extraction is done by a new hybrid deep feature learning method that integrates both the deep learning network called Enhanced Convolutional Neural Network (CNN) and Speeded Up Robust Features (SURF). With these hybrid features, feature matching is accomplished by the improved technique termed Adaptive Threshold-based Reserved Generalized Two Nearest Neighbourhood (G2NN) Feature Matching (AT-RG2NN-FM). The significant intention of the implemented scheme is to perform the optimal feature matching to attain the maximum detection rate. The performance of CNN and feature matching is enhanced by an Intermixed Forest and Cuckoo Search Algorithm (IFCSA). The experimental validation proves the effectiveness of the developed model.

Keywords: *Copy-Move Image Forgery Detection; Hybrid Deep Feature Learning; Adaptive Threshold-based Reserved G2NN Feature Matching; Intermixed Forest and Cuckoo Search Algorithm;*

1. Introduction

Photoshop is the image editing tool that is mainly used in rapid technologies to modify digital images. The degree of realism is high in the modified digital images by using the tool Photoshop [1]. In digital images, integrity as well as authenticity are protected for avoiding misleading behaviors such as duplication, fraud, information theft and copyright disputes [2]. In the modern era, there are huge types of software developed for image processing applications, and these applications are accessible, and hence unauthorized entities may easily share and modify online images. Image tampering provides significant harm to our society. The most widely adopted image tampering techniques are copy move, splicing, and manipulation removal over digital images [3]. The most relevant image forgery manipulation is the copy-move in digital images. In this forgery identification, the similarity present in the images is initially determined and then established the interrelationship between the past portion of the images and the genuine parts of the image. Among all the types of image forgery approaches, it is the easiest form, and it has the ability to add or hide meaningful objects from the same digital images. The implementation of this approach is very easy, however, the detection of images is difficult in the copy-move techniques [4]. The unusual features are searched to achieve the forgery detection approach, and the disorders or properties as the shreds of evidence. The operation of forgery detection is done with the support of homogeneity of the geometrical, physical and statistical properties of the actual images. But, the homogeneity of the original images is not managed appropriately in the tampered images [5].

A huge number of approaches have been developed for forgery detection, but these approaches require automatic feature extraction to provide effective detection outcomes. Hence, the machine as well as deep learning, has broad scope in the forgery detection field [6]. Logistic regression is a very much relevant learning-based procedure. Therefore, these regression-related procedures are considered as the building blocks for pre-processing of shared data in machine and deep learning [7]. The feature matching stage requires more time and the accuracy of the tampered locations is poor; hence it is not suitable for practical requirements [8]. The forgery detection schemes require figuring out the tampered regions in practical forensics applications. The issues such as dependability and authenticity are stated as copy-move forgery identification, and it is the key technology in digital image identification. The recently developed copy-move-based forgery identification model does not satisfy the scalable issues, and it consumes large processing times during the running analysis of large batches of images [9]. Furthermore, the large processing time and scalable conditions will cause incidental homogeneity concerns, spurious correlations, and noise accumulation. Hence, it is

[1] *GITAM School of Technology*
GITAM (Deemed to be University) Visakhapatnam
ch.saipratheek@gmail.com
[2] *GITAM School of Technology*
GITAM (Deemed to be University) Visakhapatnam
** Corresponding Author Email: giduturisrinivasarao74@gmail.com*

a need for an accurate and efficient copy-move forgery identification approach [10].

The copy-move image forgery identification approaches determine the similar regions of other images [11] [12]. Here, the strong evidence among the source regions and tampered regions are a significant consideration in copy-move image forgery detection schemes. The most commonly used algorithms for detecting forgeries are CNN, SURF, and Support Vector Machine (SVM). The significant phases included in these approaches are extraction, description, and matching of features. Many of the forgery identification models provide image authenticity and integrity [9]. Several models concentrate attention on forensic issues, and few of them are adopted for camera model recognition [13]. The matches feature points calculation is an important aspect of forgery detection schemes [14]. The detection and classification problems in the traditional forgery detection models are solved via the CNN-based forgery detection model by the automatic extraction of features [15]. The training is complicated in several complex background datasets [16]. In addition, the modification in images, such as compression, filtering, and resizing or content manipulations, are unpredictable in these approaches [17]. Robust forgery detection schemes are necessary with respect to all known manipulations [4].

The important aspects of the investigated deep learning-assisted copy-move forgery identification models are elucidated as follows.

- To propose a copy-move forgery identification scheme with the assistance of deep learning to figure out the pasted parts and replicated parts of the images.
- To develop an IFCSA for optimal tuning of Descriptors match threshold from RG2NN-FM for improving the performance of keypoint matching.
- To implement an AT-RG2NN-FM for finding the feature matching between the images to identify the forged images, where the parameter optimization takes place to improve detection performance.
- To validate the effectiveness of the employed deep learning-assisted copy-move forgery detection scheme, several heuristic algorithms and baseline works are considered.

The remaining portions describe the employed deep learning-assisted copy-move forgery identification scheme and are summarized as follows. The traditional copy-move forgery detection model with its features as well as disadvantages is given in Portion II. The architectural explanation of the proposed copy-move forgery detection scheme, proposed IFCSA description and the illustration of datasets are summarized in Portion III. The SURF and deep feature extraction with feature concatenation are listed in Portion IV. The developed AT-RG2NN-FM for feature matching to identify forged images is given in Portion V. The result analysis is provided in Portion VI and the conclusion is described in Portion VII.

2. Literature survey

2.1 Related Works

In 2020, Dhivya et al. [18] have proposed SURF feature extraction SVM object recognition for performing copy-move forgery detection. Effective impersonation forgeries have been attained by applying scaling, compression, turning, darkening, and noise addition over the images. Here, the bicubic and crop operations were used for feature matching in the developed scheme. Then, the wavelet decomposition was subjected to differentiate the forged and original images. After, the classification has done via SVM through the recognition of objects to extract similar feature points. The forgery images were detected through blending, scaling, and joint operations. The test outcomes were shown that the forged images were efficiently detected by the proposed forgery detection method.

In 2020, Diallo et al. [19] have proposed a learned feature-based forgery identification approach by visualizing the layer very deeply. Visualization-based detection model has provided efficient and robust outcomes. The CNN model has been used for learning the features from the images. Here, the CNN was subjected to the mixed quality of uncompressed and compressed images. The implementation outcome was depicted that this procedure enhanced the detection performance when contrasted to the previous approaches.

In 2020, Abhishek et al. [20] have demonstrated a forged pixel extraction and localization approach using machine learning and deep learning algorithms. Here, the "Scale-Invariant Feature Transform (SIFT) with K-Nearest Neighbor (KNN)" has been utilized for detecting the forged key points, and the classification has been done to attain the localization via SVM in machine learning structure. But, in the deep learning-based technique, the CNN has been used for extracting the features, and the forged pixels were localized through semantic segmentation algorithms.

In 2020, Chen et al. [21] have recommended a clustering-based detection technique for copy-move forgeries, where the SIFT key points were considered initially to search the unique neighborhoods, and then the tampered regions were located. On the basis of color and scale, the key point clustering has done and then it was grouped into smaller clusters to perform matching separately, which has reduced the time complexity and high dimensionality issues of SIFT. After, the pixel level tampered region localization has done via a localization algorithm, which compared the matching pairs with unique neighborhoods regarding similarity measures, and localized the pixels. Three different datasets were considered for analyzing the performance, and the results demonstrated its robustness and the forgery location accuracy, detection reliability and matching time complexity of the proposed model was high when compared to traditional algorithms.

In 2020, Zhu et al. [22] have proposed an Attention-based Residual Refinement Network (AR-Net) based on a neural network to detect the copy and move forgeries by fully capturing the context information. The self-correlation between feature maps has been computed through deep matching of features, and the scaled correlation maps were fused via "Atrous Spatial Pyramid Pooling (ASPP)" in order to create a coarse mask. In addition, the residual refinement module has been used for optimizing the coarse mask that retained the constitution of the object's boundary. The COVERAGE, CoMoFoD and CASIAII proved the robustness of the proposed AR-Net on post-processing operations like blur, noise, and JPEG recompression.

In 2019, Agarwal et al. [23] have proposed a copy-move forgery identification approach with high efficiency using deep learning. The processing steps to be involved in the proposed model were segmentation, retrieval of features, reconstruction of dense depth region, and tampered area identification. The morphologically affected image has been identified through the proposed mechanism. The images were duplicated from one particular place to another location, where distinct transformations like scaling, noise formation, blurring, rotation, and compression were used for examining the tampered location of the images. The computation time has highly decreased and the duplicated regions of the images were effectively detected using the proposed mechanism.

In 2020, Elaskily et al. [24] have suggested a deep learning-based innovative design for detecting the copy-move forgeries automatically. From the input images, the hierarchical feature representations were learned by CNN for detecting forged images. The learned features were useful for the detection of tampered and original images. At last, the empirical analysis outcomes were shown that the proposed model outperformed the traditional models among various benchmark data sources in regards to accuracy and system robustness.

In 2020, Elhaminia et al. [25] have proposed a novel copy-move forged image identification by using Markov Random Field. Here, the segmentation approach has been performed to gain a proper balance between speed and precision. The posterior labeling has been maximized by the intelligent selection of binary and unary potentials on the forged regions. The quantitative and qualitative tests have been conducted over benchmark datasets to validate the efficacy, and the performance of the implemented forgery identification scheme was superior to the traditional approaches.

2.2 Problem statement

The identification of copy-move forgery approaches can effectively identify and locate the tampered regions. However, most of the methods are still defective in the detection of copy-move forgery. Numerous copy-move forgery detection techniques are tried to improve their performance, which is reviewed in Table 1. SVM [18] has high detection accuracy and the overall performance is improved by selecting the strongest points from the input images. However, it doesn't provide accurate results when it is applied to recognize objects in video images.CNN [19] gives promising results by proposing a highly robust model for camera and image forgery detection. However, the overall performance is lacking when it is applied to multiple image manipulations. DCNN [20] improves accuracy in the detection of forged pixels by classifying the image pixels and localizing them. However, the time consumption is high for pre-processing. Key-point clustering [21] improves the efficiency of forgery detection, has greater robustness, and it places the tampered portions accurately. However, this method is not suitable for large-scale forgery. AR-Net [22] has greater robustness in the operations of post-processing. However, it doesn't utilize the information of multiple modes since it is single-stream. VGGNet [23] improves accuracy by removing the unforged regions from the real forged regions. However, it does not have the ability to identify the forged image using a Multi-cloned attack. CNN [24] improves accuracy by the automatic extraction of image features, and it constructs feature maps. However, it takes more transition time when the number of datasets increases. Markov Random Field [25] identifies the forged regions with acceptable accuracy. However, it is not suitable for post-processing functions. The experimental results revealed that the developed approach identify the duplicated images effectively with higher detection accuracy. The reported results suggest that the proposed method can detect forged regions efficiently and with acceptable accuracy. In addition, image forgery detection approaches using deep learning will identify various types of forgeries in the future.

Table 1. Benefits and challenges of Existing copy-move forgery detection models using deep Learning

Author [citation]	**Methodology**	**Features**	**Challenges**
Dhivya *et al.* [18]	SVM	High accuracy was achieved through this technique. The overall	This technique doesn't provide accurate results when it is applied

		performance is improved by selecting the strongest points from the input images.	to recognize objects in video images.
Diallo *et al.* [19]	CNN	This technique gives promising results by proposing a robust model for image forgery detection and camera identification.	The overall performance is lacking when it is applied over multiple image manipulations.
Abhishek *et al.* [20]	DCNN	The overall accuracy in the detection of forged pixels is improved by classifying the image pixels and localizing them.	In this model, the training time and computation complexity are very high.
Chen *et al.* [21]	Key-point clustering	This method reduces the matching time and improves the forgery detection efficiency. It has greater robustness, and it locates the tampered portions very efficiently.	This method is not suitable for large-scale forgery.
Zhu *et al.* [22]	AR-Net	This method has high robustness in post-processing operations.	It doesn't utilize the information of multiple modes since it is single-stream.
Agarwal *et al.* [23]	VGGNet	The accuracy is improved by removing the unforged regions from the real forged regions.	This method does not detect the image forged using a Multi-cloned attack.
Easily *et al.* [24]	CNN	The accuracy of this method is improved by the automatic extraction of image features and the constructs feature maps.	It takes more transition time when the number of datasets increases.
Elhaminia *et al.* [25]	Markov Random Field	This method efficiently detected the forged regions with acceptable accuracy.	This method is not suitable for post-processing operations.

3. Implementation of Copy-Move Forgery Detection Scheme using Adaptive Deep Feature Learning and Collection of Datasets

3.1 Primary Description of Proposed Model

Copy-move forgery identification is the most popular research in recent years, and more technologies are employed for solving the issues aroused during the identification of copy-move forgeries. Here, the extraction of features and learning-based approaches provide higher feature matching, and it requires some post-processing techniques to improve the learning ability with no error. Hence, it takes more time while identifying the copy-move forgeries. Key point-based feature extraction techniques are needed to identify the unique features. But, the texture matching-related techniques suffered from dimensionality issues and hence the dimension reduction techniques are required to decrease the input dimension. Most of the techniques focused on improving the system's accuracy, but they should not concentrate on system robustness. In addition, the traditional deep learning-based copy move forgery identification approaches are suffered from higher computational complexity because the matching of huge identical points in the image is slightly complex. The traditional approaches are less effective in smooth and homogeneous regions. Therefore, a new detection model for detecting copy-move forgeries is needed to identify the forged images with higher accuracy and less complexity. The structural description of the proposed copy-move forgery detection model using deep learning is illustrated in Fig. 1.

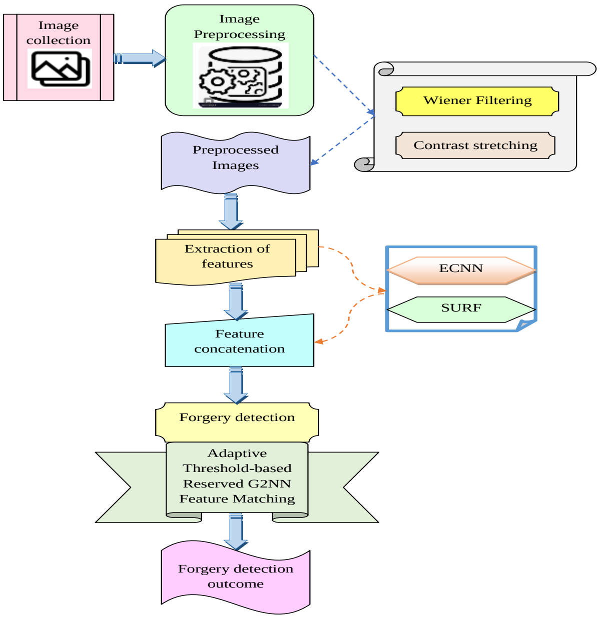


Fig 1. Block schematic representation of proposed copy-move forgery detection model using deep learning

A new feature matching-based copy-move forgery identification model is developed using deep learning for detecting duplicate images for preventing the intention of malicious users in social media. The images required for identifying the copy-move forged images are taken from two distinct datasets at first. The preprocessing algorithms are applied to the collected images to enhance the image quality without degrading the image information. In this preprocessing stage, the wiener filtering and contras enhancement techniques are assisted in enhancing image quality. The features from the preprocessed images are retrieved using CNN-based deep feature extraction and SURF-based feature extraction. The retrieved deep and SURF features are concatenated to get the combined feature. The concatenated feature is given to the AT-RG2NN-FM for identifying the matching point between the pixels from the two images for identifying the forged images. The descriptor match threshold parameter is tuned from the AT-RG2NN-FM with the support of the proposed IFCSA to enhance the detection performance. The forgery identification effectiveness of the implemented feature matching-based copy-move forgery detection model using deep learning is ensured over the conventional forgery identification approaches while concerned with several detection metrics.

3.2 Image Collection

The copy-move forgery detection images are acquired from the "CoMoFoD - Image Database for Copy-Move Forgery Detection" dataset with the source of "https://www.vcl.fer.hr/comofod/ accessed on 2023-08-07". The CoMoFoD dataset is used for the identification of copy move forgeries and it contains 260 forged sets of images. There are two categories of images presented, small and large. The size of large images is 3000×2000 and the size of small images is 512×512. According to the applied manipulation like rotation, translation, scaling, distortion and combination, the images are grouped into 5 classes.

The name of dataset 2 is "Copy-Move Forgery Detection and Localization," and it is obtained from the link of "http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/ with the access data on 2023-08-09". The datasets present in the source are "MICC-F220, MICC-F8multi, MICC-F2000, and MICC-F600". MICC-F220 comprised 220 images, where 110 are tampered images and 110 are original images. MICC-F2000 is composed of 2000 total images, where 1300 are original images and 700 are tampered images, MICC-F8multi comprised of 8 tampered images and MICC-F600 comprised of 440 images, where 160 are tampered images and 160 are original images.

The sample images obtained from online sources for detecting copy-move forgeries are given in Fig. 2.

Image description	1	2	3	4	5
Dataset 1					

Dataset 2					”

Fig 2. Sample images obtained from the online sources for detectingcopy-move forgeries

The collected images required for the identification of copy-move forgeries are indicated by the term CM_x^{OR}, which $x = 1,2,...,X$ represents the total count of images.

3.3 Image Preprocessing

The image processing methods are applied to suppress the distortions in the images for improving the image features. The complexity of copy-move forgery identification is reduced, and the processing speed is also enhanced by using preprocessing techniques. The wiener filtering and contrast enhancement techniques are applied to preprocess the images.

Wiener filter [26]: The collected CM_x^{OR} images are given to wiener filtering for reducing the noise. It is a type of low-pass filter, which is substituted in distinct contexts to restore the noise-degraded signals. On the basis of statistical approach, the filter assumes the noise and the signal are stationary linear stochastic with respect to relevant spectral characteristics. It strikes the optimal imbalance, and hence the performance of this process is superior in its bias-variance tradeoff. The mean and variance of the neighborhood is estimated by the wiener filter and hence it is called an adaptive filter. Then, subjects the minimal and strong smoothing based on high and low variations.

The error between the original and estimated signal is minimized by using this filter and this is expressed in Eq. (1).

$$Er^2 = Ex\left\{\left(k - \hat{k}\right)^2\right\}$$
(1)

Here, the term k represents the uncorrupted image and the term $\hat{k}$ is the estimated images and $Ex\{\cdot\}$ is the argument's expected value. The minimum quadratic error of the estimated image is obtained by considering the assumption as, the image or noise is zero mean, the image as well as the noise are uncorrelated, and the estimated image's intensity level is degraded by the linear function, which is illustrated in Eq. (2).

$$\vec{K}(m,n) = \left[\frac{D^*(m,n)P_k(m,n)}{P_k(m,n)|D(m,n)|^2 + P_k(m,n)}\right]C(m,n) \tag{2}$$

In the frequency domain, the estimated image is indicated as $\vec{K}(m,n)$, the degradation function transformation is denoted as $D(m,n)$, $D^*(m,n)$ is the complex conjugate function, $C(m,n)$ is the degraded image transformation and $P_k(m,n) = |K(m,n)|^2$ is the non-degraded image's power spectrum. The multiplication of complex value and its conjugate is the general principle of the filter that is given in Eq. (3).

$$\vec{K}(m,n) = \left[\frac{1}{D(m,n)} \frac{|D(m,n)|^2}{|D(m,n)|^2 + \frac{P_\eta(m,n)}{P_k(m,n)}}\right]C(m,n) \tag{3}$$

Here, the term $P_\eta(m,n)$ is the noise power spectrum of the images. The intensity of the images is degraded due to the constant power additive noise and this problem is solved by the use of a wiener filter. The filtered noise output is denoted by CM_x^{WF} .

Contrast stretching [27]: The noise-reduced images CM_x^{WF} are given to the contrast enhancement process. It is a contrast enhancement technique that is utilized for improving image contrast. The main types of contrast stretching are linear and global contrast stretching. Here, the global contrast stretching method manifests them in the fashion of global like the poor or excessive condition of lighting in the source environment. It highly improves the image from the luminance information, and high global contrast may cause a variation-rich and detailed global feeling of the image. However, the lower global contrast consists of fewer details and less information, and it appears to be unique. The global contrast stretching process is given in Eq. (4).

$$O_{RGB}(m,n) = 255 * \left[\frac{D_{RGB}(m,n) - \min_{RGB}}{\max_{RGB} - \min_{RGB}}\right] \tag{4}$$

The original RGB pixel value is denoted by $D_{RGB}(m,n)$ and the newly attained value of pixel coefficient is indicated as $O_{RGB}(m,n)$. The minimum and maximum values among the RGB pixel values are denoted by $\min_{RGB}$ and $\max_{RGB}$ correspondingly.

In the local contrast stretching process, the stretching process is done for each RGB component. The stretching amount is subjected to the neighborhood, and it is limited by the original contrast of the images, which is expressed in Eq. (5).

$$O_{RGB}(m,n) = 255 * \left[\frac{D_{RGB}(m,n) - \min}{\max - \min}\right] \tag{5}$$

The original and output of RGB components are denoted by the terms $D_{RGB}(m,n)$ and $O_{RGB}(m,n)$. The minimum and maximum value of each component is indicated by $\min$ and $\max$, correspondingly. The contrast-enhanced images are indicated by CM_x^{CE}.

4. Hybrid Deep Feature Learning-based Deep Feature Extraction for Getting Key Points from Images

4.1 Basic CNN

The deep features from the preprocessed images are attained using the ECNN technique. The contrast-enhanced images CM_x^{CE} are given to ECNN for extracting deep features.

ECNN [28]: It is a type of Deep Neural Network (DNN) and it is constructed on the basis of layer-by-layer. Features from the input images are extracted through four types of layers. The convolutional layer checks the connected output neurons to the input. Then, the input of the convolutional layer is denoted by $u \times v$. The height and width of the matrix are denoted by u and v correspondingly. The dimension of the matrix is lesser than the dataset, where the size of the kernel is utilized as filter size. The feature mapping function is given by this filter size. The connected structure is provided by the filter size and the ReLu is the activation function, which is expressed in Eq. (6).

$$\mathrm{Re}\,Lu(y) = Max(0, y) \tag{6}$$

The matrix with small values is provided by the maximum pooling layer in the network, which prefers the greatest values from distinct matrices. The padding, input size and number of filter is indicated by the terms pd s and f, respectively. It is assumed as $32 \times 32 \times 1$. The overfitting problem is eliminated by the dropout layer. All the neurons are converted into a single connected layer by using the flattened layer. The extraction of features is carried out by a dense layer. Here, all the nodes are connected to one another. The extracted deep features are indicated by DF_x^{CE}.

4.2 Basic SURF

The preprocessed images CM_x^{CE} are given to SURF for the extraction of SURF features. In this developed model SURF [29] is used for extracting the features without reducing the image quality over the identified points. Thus, the scale space is introduced with the different size box filters and then convolutes with the integral images. The applied image is denoted as $CM = (u,v)$ and the Hessian matrix $Hs(u,\kappa)$ in u at scale κ is illustrated in below Eq. (7).

$$Hs(u,\kappa) = \begin{bmatrix} Cn_{uu}(u,\kappa) & Cn_{uv}(u,\kappa) \\ Cn_{uv}(u,\kappa) & Cn_{vv}(u,\kappa) \end{bmatrix} \tag{7}$$

The convolution result is denoted by $Cn_{uu}(u,\kappa)$, and the second order derivative of the image $CM = (u,v)$ is denoted by $Cn_{uv}(u,\kappa)$ and $Cn_{vv}(u,\kappa)$ in point u.

Here, the non-maximum suppression and Hessian matrix are used to detect the potential key points. Finally, the extracted features using SURF are indicated by DF_m^{Surf}.

4.3 Feature Concatenation

The extracted deep features from ECNN DF_x^{CE} and SURF features DF_m^{Surf} are given to the feature concatenation process. The feature extraction enhances the instability of the network and enhances the accuracy of the model. The concatenated features improve the detection efficacy in terms of decreased computational complexity. The overfitting issues are effectively solved with the help of this feature concatenation process. In addition, the dimensionality issues are also solved with the help of this feature concatenation process. The concatenated features are represented by Co_g^{fs}. The structural illustration of feature extraction with feature concatenation is given in Fig. 3.

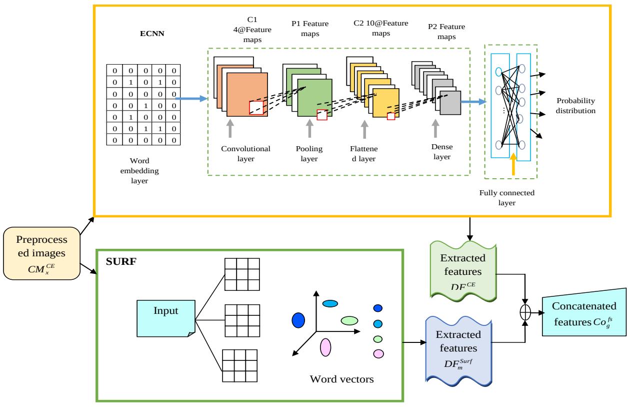


Fig 3. Structural depiction of feature extraction and feature concatenation

5. Copy-Move Forgery Detection Through Nearest Neighbor-based Feature Matching with Optimal Tuning of Parameters

5.1 Developed IFCSA

The implemented IFCSA is used in the implemented copy-move forgery identification approach for optimizing the descriptor match threshold during feature matching. The optimized threshold value improves the detection performance. The position is updated using the developed concept in the proposed IFCSA. The conventional FOA algorithm seeding operator and CSO algorithm position are used for the implementation of the proposed IFCSA. The final position of the developed IFCSA is illustrated in Eq. (8).

$$Po = Old_{Po} + s\tan d\left(\frac{No_{\text{var}} + V_m^{(r+1)}}{50}\right) \tag{8}$$

The term Po is the new position to be calculated in IFCSA, Old_{Po} is the old position obtained from the previous step, the seeding parameter of the FOA algorithm is indicated by No_{var}, the updated position is represented by $V_m^{(r+1)}$ and the standard position is denoted by the term $s\tan d$. The results proved that the convergence rate of the designed IFCSA is greater when contrasted to the traditional algorithms. A better solution is obtained by using the proposed IFCSA.

FOA [30]: It is an evolutionary algorithm that is suitable for solving continuous optimization problems and it is inspired by the trees. The main stages involved in the FOA are trees' local seeding, population limitation and trees' global seeding. The potential solution of the problem is represented by all the trees. First, the tree's age is set to '0' and the local seeding operator generates the new trees after initialization. Previously generated trees are assumed as old ones except the newly generated key. After, there is a population control, where some trees will be omitted and this population is given to the global seeding stage. Some new potential solutions are added in the global seeding stage for getting rid of local optimum solutions. Finally, the ranking is provided to the trees based on the fitness values in the forest.

Trees initialization: The potential solution of all problems is taken as tree and all the trees depict the variable values. The age of each tree is considered as 0 and it is increased after generating the new trees in the search space. The tree can be represented in the array format, where the age of the related tree is denoted by Age Eq. (9).

$$Tree = \lfloor Age, v_1, v_2, ..., v_{No_{\text{var}}} \rfloor \tag{9}$$

The predefined parameter is used for representing the maximum age of the tree. The dimension of the problem is indicated as No_{var} and the length of the array is assumed as $1 \times (No_{\text{var}} + 1)$. Initially, the $lifetime$ parameter is determined and the value of this is changed according to the omission of trees from the forest.

Local seeding of trees: The seeding procedure starts when the trees begin to fall, and after some time, they turn into younger ones. Then, the competition among the neighborhood trees is started based on the condition of sunlight and location. The predefined parameter is used for providing the value of the local seeding tree and it is called as local seeding change (LSC). The number of generated trees and the total count of trees after seeding the local stages are determined through LSC. This generates the random number in the range between $[1, No_{\text{var}}]$.

Control of population: The expansion of forests is limited by limiting the population stage. At first, the total amount of trees present in the forest is the same as that of $area\lim it$. Two steps are involved in the limiting population phase, where the initial step is to eliminate the trees in the forest they intersected $lifetime$ and then the rejected trees are inserted into the candidate population. At last, the trees are arranged on the basis of fitness value in the second step in descending order.

Global seeding of trees: In the original population of candidates, some amount of population is applied in the stage of global seeding of trees. The transfer rate parameter is defined for denoting the share that is utilized to global seed. Another predefined parameter used in this stage is Global Seeding Changes (GSC) in the FOA. The global seeding procedure is subjected to some trees only. Finally, the newly created tree is also included in the forest.

Updating the best tree: Based on the fitness value and classification process, the trees are arranged. Then, update the age of the best tree to 0 because of without causing age limited issues. The seeding of local tree can be done to the tree having 0 values, which is useful for the optimization of best solution.

CSO [31]: It is Metaheuristic, nature inspired algorithm that is functioned on the basis of cuckoo species' brood parasitism along with the random walks of Levy flights. Animals choose the quasirandom or random manner for searching their food in nature. Animals randomly walk in the foraging behavior and then it changes the location on the basis of location of current state and probability of transition. Generally, the random walk is assumed for levy flight, where the levy flights are evaluated based on the probability distribution of heavy tails. After processing several steps, the random walk distance from the origin leads to a stable distribution.

The solution in the problem space is indicated by each egg in the nest, and the new occurred solution is denoted by cuckoo egg. For employing the new and better solutions, not-so-good eggs are replaced from the nest. Simply it is stated as each nest has one egg. The new solution generation based on Levy flight distribution of CSA is represented in Eq. (10).

$$V_m^{(r+1)} = V_m^{(1)} + \vartheta \oplus Levy(\varsigma) \quad (10)$$

The generated new solution is represented as $V_m^{(r+1)}$ and the old solution is signified as $V_m^{(1)}$. The step size related to problem scale is denoted as ϑ and the levy flight distribution in problem space is indicated by $Levy(\varsigma)$, where $(1 < \varsigma \le 3)$.

In CSA, the habitat of cuckoo is considered as an array of $1 \times M_{\text{var}}$, where M_{var} indicates the dimensionality of the problem. The array of habitats is defined as follows $[v_1, v_2, ..., M_{\text{var}}]$, where each variable is considered to be a floating point number. The profit of evolution is estimated with respect to the habitat array. This profit function is useful for evaluating the cost function value. To minimize the cost function, the profit function value should be high. The size of the habitat matrix of the candidate is denoted by $M_{popn} \times M_{\text{var}}$ and it is created in the initial stage of the algorithm. The maximum range of cuckoo's laying their eggs is denoted as Egg Laying Radius (ELR). This radius is evaluated through the upper and lower limit of the variables. ELR is the ratio of the total count of eggs in the nest to the count of eggs for the cuckoo, which is formulated in Eq. (11).

$$ELR = \vartheta \times \left(\frac{Current\,number\,of\;cuckoo's\,eggs}{Total\,number\,of\;eggs\,in\,the\,nest} \right) \times \left(\text{var}_{up} - \text{var}_{lw}\right) \quad (11)$$

The upper limit is denoted by var_{up}, the lower limit is signified by var_{lw} and the term ϑ is the integer that is used for getting the maximum value of ELR.

All the cuckoos lay eggs randomly in some other nest of the host bird. After laying eggs in the other bird's nest, the host bird throws out the egg of the cuckoo. Therefore, the profit values have been decreased.

The young cuckoos grow and live in their own area and society. The egg-laying behavior has immigrated the new and better habitats and provides food to their youngsters. The best profit value cuckoo bird is selected as the goal point in the society and hence the other birds to immigrate. The nearest cuckoos in the society are grouped together by using the K-means Clustering (KMC) procedure. Then, the mean profit value is evaluated, which is helpful for achieving the goal group and best destination habitat.

The predators kill the cuckoos for food and hence the population of the cuckoo birds is limited. Only a small number of cuckoos with the best profit values live in society. The pseudocode of the designed IFCSA is shown in Algorithm 1. The step-by-step diagram is demonstrated in Fig. 4.

Algorithm 2: Developed IFCSA

```
Start IFCSA
Load the population parameters in FOA and CSO
Set the count of the population of CSO
Set the maximum number of the iteration count
While $(q < stopping\,criteria)$
Ensure the fitness in problem space
For $n = 1\,to\,A$
For $m = 1\,to\,B$
  Find the seeding operator in FOA
  Find the position of cuckoos in CSO
    Update the position of IFCSA using the newly implemented concept in Eq. (8).
Attaint the best solution
End for
End for
End while
End
```

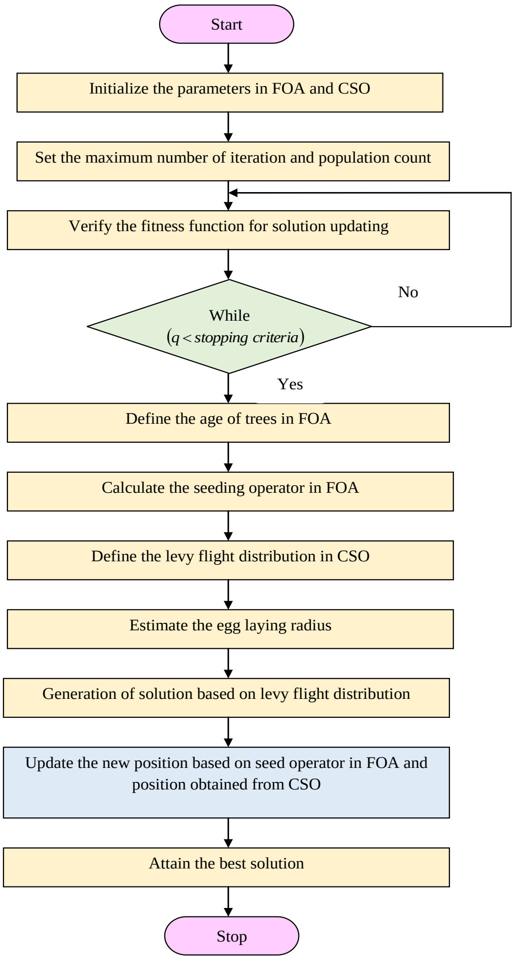

Start
Initialize the parameters in FOA and CSO
Set the maximum number of iteration and population count
Verify the fitness function for solution updating
While
(q < stopping criteria)
No
Yes
Define the age of trees in FOA
Calculate the seeding operator in FOA
Define the levy flight distribution in CSO
Estimate the egg laying radius
Generation of solution based on levy flight distribution
Update the new position based on seed operator in FOA and position obtained from CSO
Attain the best solution
Stop

Fig 4. Step-by-step diagram of IFCSA

5.2 Basic RG2NN

The concatenated features Co_g^{fs} are given to the G2NN [29] for the description of features. The matching between two images is determined by using the nearest neighbor concept. Here, the multiple copies of the same copies are detected through G2NN algorithm. The Euclidean distance between two images is calculated using the G2NN criteria. The Euclidean distance between the descriptors is given in Eq. (12).

$$\lambda_{co} = \{Eu_{co,1}, Eu_{co,2}, ..., Eu_{co,m}\} \tag{12}$$

Here, $\lambda_{co,m}(co, m = 1,2,...,k; co \neq m)$ is defined as the Euclidean distance among the images. The similarity between the descriptors is estimated based on the Euclidian distance square and it is given in Eq. (13).

$$Eu_{co,m} = \left\| Fs_{co}^{extr} - Fs_{co}^{org} \right\|_2 \tag{13}$$

On every row of the distance matrix, the 2 nearest neighbors are iterated for determining the multiple copies. The iteration stops based on the condition λ_{co}.

$$Eu^2_{co,m} / Eu^2_{co,m+1} < Thr \tag{14}$$

Here, the term Thr indicates the threshold parameter and the iteration is terminated when the key point corresponding to the distance is $\{Eu^2_{co,1}, Eu^2_{co,2}, ..., Eu^2_{co,l}\}$, where $l = 1,2,..k, l \neq co$. RG2NN is the enhanced version of G2NN, where the proportion of nearest and second nearest neighbor is considered. The Euclidian distance between the neighbors are arranged in reversed order based on the other key points. The final key point matching is carried out with respect to threshold values. The ratio is smaller then considers two random features are there if the ratio is greater and it has the ability to match key points. In this way, the key point descriptors are identified using G2NN architecture. The basic structure of G2NN is depicted in Fig. 5.

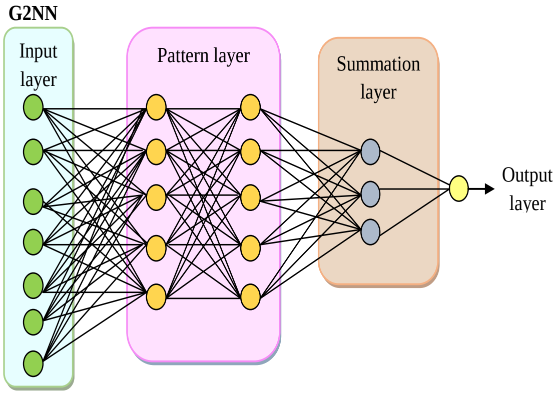


Fig 5. Basic structural description of G2NN

5.3 Copy-Move Forgery Detection using AT-RG2NN-FM

The matching of key points between two images is mainly depending on the threshold parameter Thr. The ratio between the threshold parameter and distance is decreased, and hence the matching accuracy is highly increased. The set of threshold points is used for determining the number of matched pairs and mismatched pairs for the detection of forged images. The descriptor match threshold value is optimized via the proposed IFCSA in the developed copy-move forgery identification model. The optimal selection of descriptor match threshold value during feature matching improves the accuracy and precision. During the selection of the threshold value, two observations are made that are when we increase the threshold factor, the incorrect matches increase rapidly and correct matches tend to be constant. In addition, more false matches occurred due to a higher threshold factor. Hence, the appropriate selection of threshold values is significant for getting correct matches and the incorrect matches occur within the acceptable limits. The features are matched between the images on the basis of the tuned threshold value and after matching this, a large number of matched pairs is attained. The adjacent key points have higher similarity when compared to other pixels. The match pairs are eliminated when it satisfies the condition in Eq. (15).

$$\sqrt{(p_u - p_v)^2 + (q_u - q_v)^2} < Thr \qquad (15)$$

The coordinates of matched key points are denoted by $(p_u - p_v)$ and $(q_u - q_v)$, respectively. The threshold parameter is defined by Thr. During feature matching, the more mismatched pairs are eliminated and hence the forged images are effectively identified. The objective of the feature matching based on optimal tuning of the descriptor match threshold is expressed in Eq. (16).

$$Obj = \arg\min_{\{Thr_x^{G2NN}\}} \left(\frac{1}{ACRY + PCN} \right) \qquad (16)$$

The term Thr_x^{G2NN} represents the optimized descriptor match threshold and Obj indicates the objective of the implemented model. The accuracy of the implemented scheme is indicated by Ar and the precision of the proposed model is signified by Pn. The mathematical expression of accuracy and precision is illustrated below in Eq. (17) and Eq. (18).

$$ACRY = \frac{Xy_{pos} + Xy_{neg}}{Xy_{pos} + Xy_{neg} + Mn_{pos} + Mn_{neg}} \qquad (17)$$

$$PCN = \frac{Xy_{pos}}{Xy_{pos} Mn_{neg}} \qquad (18)$$

The true positive observation, true negative observation, false positive observation and true negative observation measure are denoted by the terms Xy_{pos}, Xy_{neg}, Mn_{pos} and Mn_{neg}. The structural description of the proposed AT-RG2NN-FM-based copy-move forgery identification process is illustrated in Fig. 6.

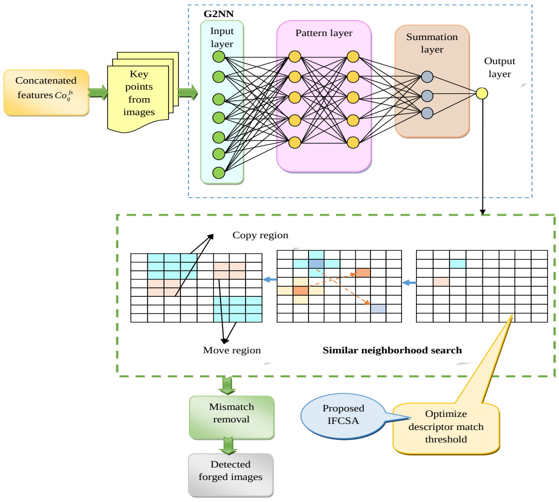


Fig 6. Basic structural description of the proposed AT-RG2NN-FM-based copy-move forgery identification

6. Results and Discussions

6.1 Experimental Setup

Python software has been utilized to implement the proposed deep learning-related copy-move forgery identification scheme, where the experimental analysis has been done to guarantee the efficacy of the proposed scheme. The number of chromosomes, population and iteration were considered as 10, 1 and 50. The traditional optimization algorithms and forgery detection methodologies were adopted for the comparison of performance. The conventional optimization algorithms, including Particle Swarm Optimization (PSO) [32], Squirrel Search Optimization (SSO) [33], FOA [30] and CSA [31], were utilized for making comparative analysis. The traditional copy-move forgery detection models like SURF [34], CNN [19], and RG2NN [35] were taken for validating the effectiveness.

6.2 Resultant Images

The copy-move forged defection outcomes are listed below in Fig. 7.

Image description		**1**	**2**	**3**	**4**	**5**
Dataset 1	Original Images					
	Ground truth images					”

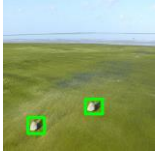
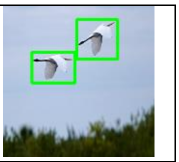
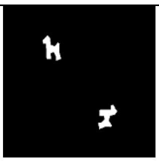
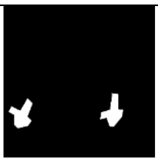
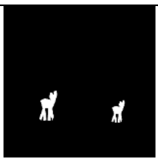
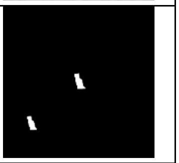
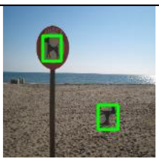
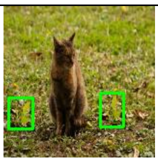
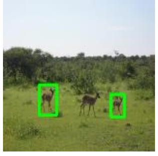
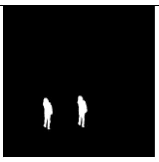
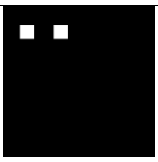
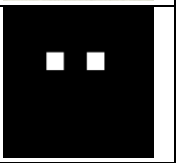
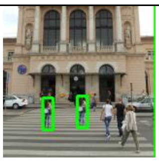
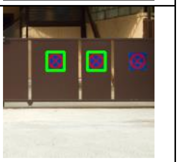
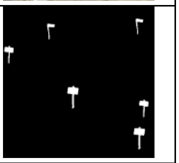
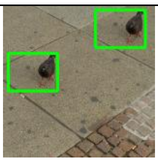
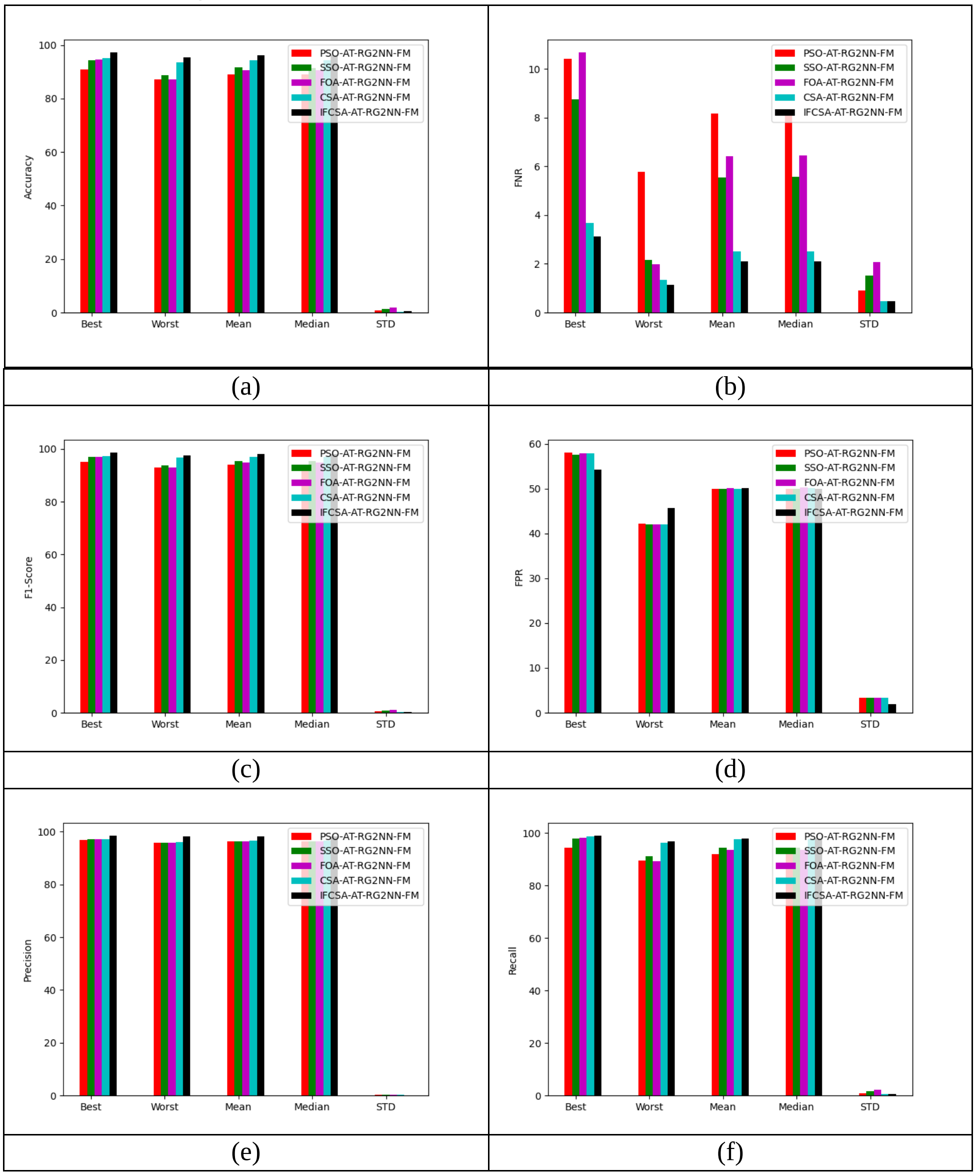
	Forged detected images					
		6	7	8	9	10
	Original Images					
	Ground truth images					
	Forged detected images					
		1	2	3	4	5
Dataset 2	Original Images					
	Ground truth images					
	Forged detected images					
		6	7	8	9	10
	Original Images					
	Ground truth images					
	Forged detected images					

Fig 7. Resultant copy-move forgery detection outcomes

6.3 Performance analysis of algorithms

The performance of the implemented deep learning-related copy-move forgery detection model is validated with respect to various heuristic algorithms in regard to several observation metrics. The dataset 1 analysis is depicted in Fig. 8 and a dataset 2 analysis is illustrated in Fig. 9. The F1-score of the developed IFCSA-AT-RG2NN-FM-based copy-move forgery detection scheme accomplished with 4.34% than PSO-AT-RG2NN-FM, 3.22% than SSO-AT-RG2NN-FM, 4.34% than FOA-AT-RG2NN-FM, 1.305%

than CSA-AT-RG2NN-FM for considering the mean statistical measure. The detection accuracy is also improved than the conventional algorithms in the proposed copy-move forgery identification scheme while considering dataset 2.

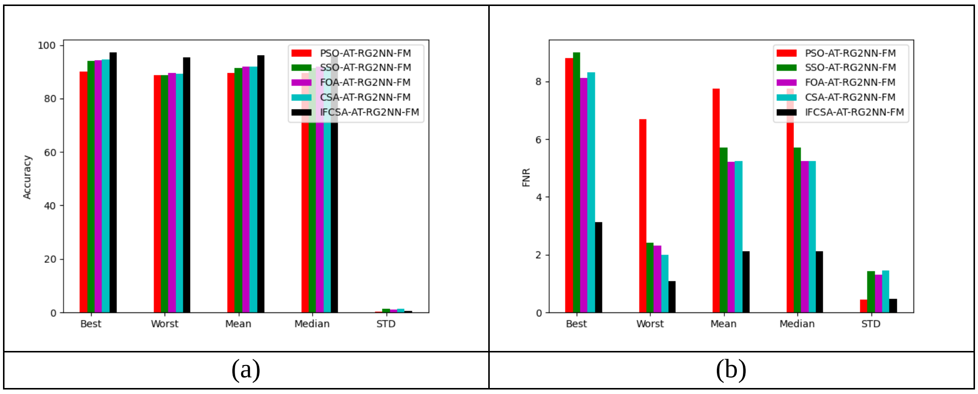


(a) (b)

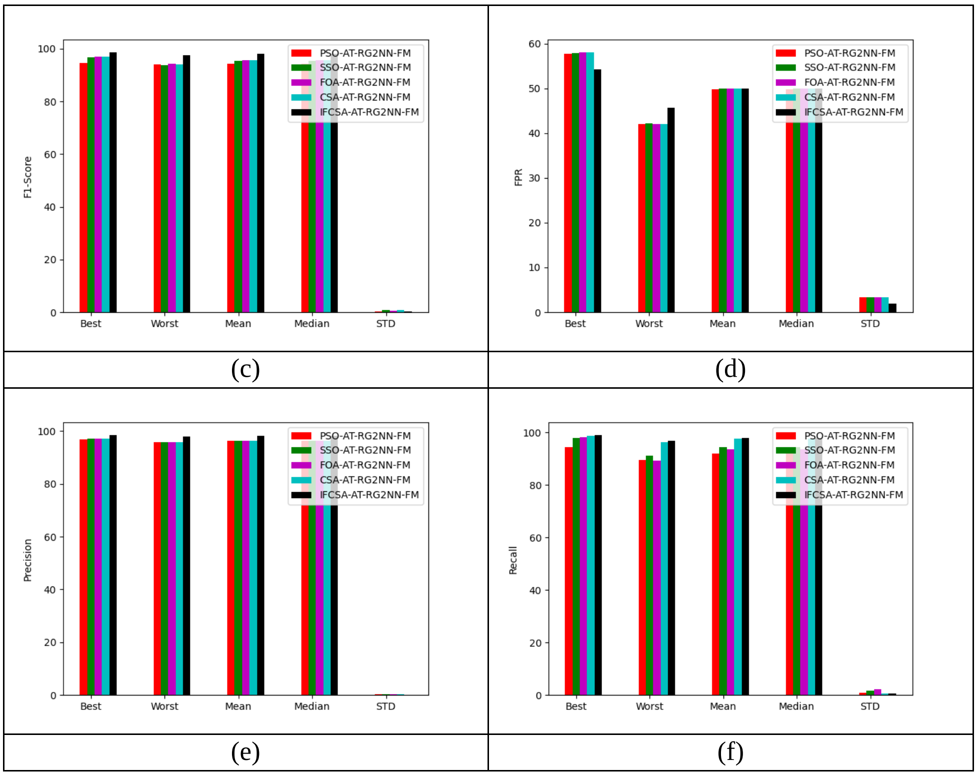
(c) (d)

(e) (f)

Fig 8. Effectiveness analysis of the implemented deep learning-based copy-move forgery identification scheme among various optimization strategies according to "(a) Accuracy (b) FNR (c) F1-score (d) FPR (e) Precision (f) Recall" among dataset 1



(a) (b)



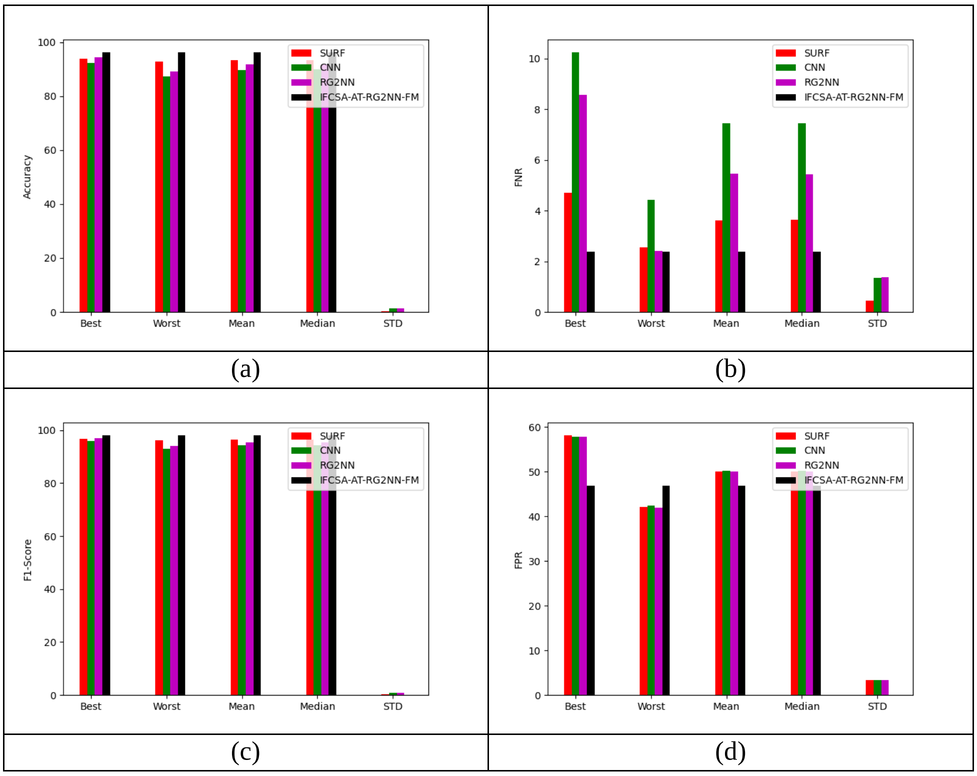
(c) (d)

(e) (f)

Fig 9. Effectiveness analysis of the implemented deep learning-based copy-move forgery identification approach among various optimization algorithms according to “(a) Accuracy (b) FNR (c) F1-score (d) FPR (e) Precision (f) Recall” among dataset 2

6.4 Performance validation among various techniques

Previously implemented copy-move forgery identification models are considered for analyzing the performance of the proposed IFCSA-AT-RG2NN-FM-based copy-move forgery identification scheme for validating its efficiency. The dataset 1 validation outcome is given in Fig. 10, and a dataset 2 validation outcome is illustrated in Fig. 11. The precision of the implemented approach is enhanced with 1.03% than SURF, 4.25% than CNN, 3.15% than RG2NN for considering the mean statistical measure. Dataset 2 also performed well while considering various statistical measures rather than the traditional copy-move forgery detection schemes.



(a) (b)

(c) (d)

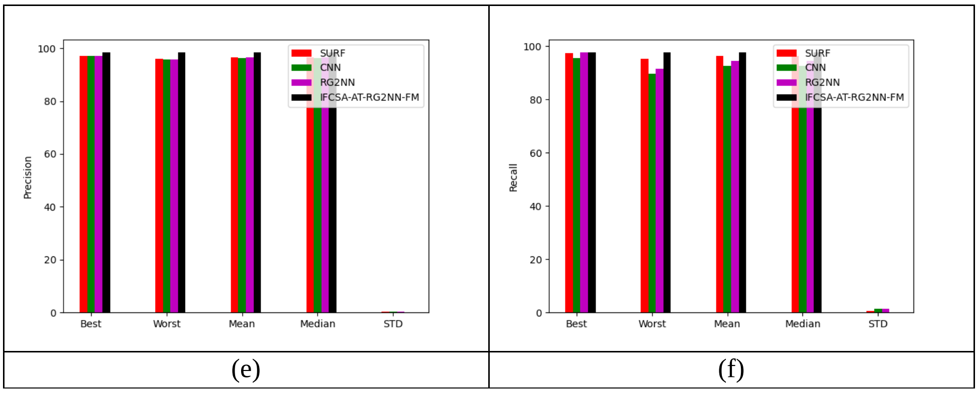


Fig 10. Effectiveness analysis of the implemented deep learning-based copy-move forgery detection scheme among previous detection models according to (a) "Accuracy (b) FNR (c) F1-score (d) FPR (e) Precision (f) Recall" among dataset 1

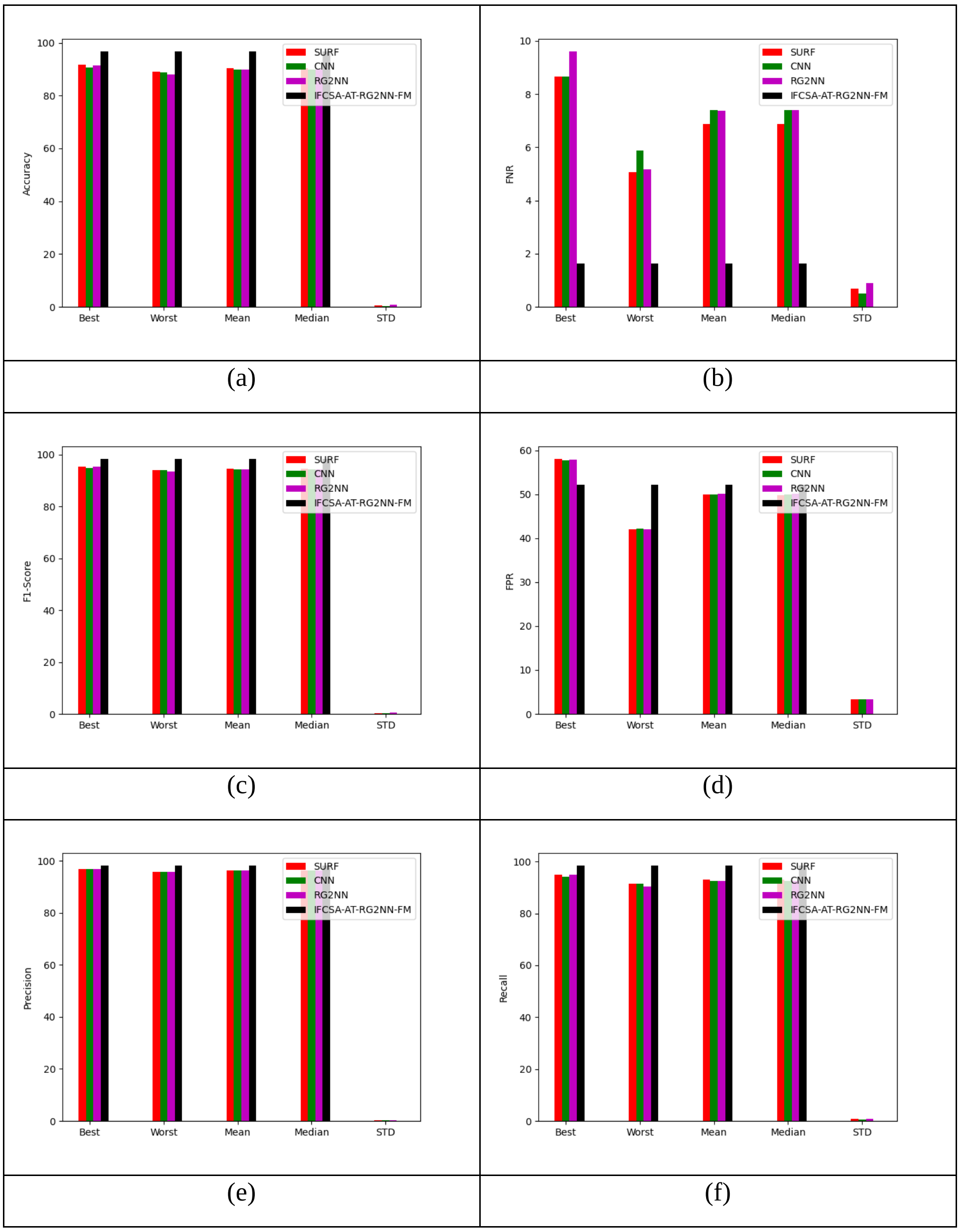


Fig 11. Effectiveness analysis of the implemented deep learning-based copy-move forgery detection scheme among previous detection models according to "(a) Accuracy (b) FNR (c) F1-score (d) FPR (e) Precision (f) Recall" among dataset 2

6.5 Performance Computation among Dataset 1 and Dataset 2

The performance comparison of the investigated deep learning-based copy-move forgery identification scheme among various algorithms and techniques are listed in Table 2 and Table 3, respectively. The MCC of the designed scheme is enhanced with 4.51% than SURF, 4.40% than CNN, and 4.14% than RG2NN for considering data set 2 in Table 3. All the performance measures are provided greater efficiency when compared to the traditional algorithms and techniques.

Table 2. Performance validation on heuristic strategies on proposed Deep Learning-based copy-move forgery detection scheme

Performance measures	PSO-AT-RG2NN-FM [32]	SSO-AT-RG2NN-FM [33]	FOA-AT-RG2NN-FM [30]	CSA-AT-RG2NN-FM [31]	IFCSA-AT-RG2NN-FM
For dataset 1					
“Accuracy”	89.09751	91.54199	90.7167	94.36561	96.27665
“Sensitivity”	91.84042	94.44415	93.58164	97.48062	97.88826
“Specificity”	96.32455	96.43463	96.38117	96.5269	98.25264
“Precision”	50.01494	49.89109	50.14905	50.00223	50.06145
“FPR”	8.159575	5.555854	6.418364	2.519384	2.111735
“FNR”	94.02612	95.42242	94.94901	97.00014	98.06951
“NPV”	89.09751	91.54199	90.7167	94.36561	96.27665
“FDR”	91.84042	94.44415	93.58164	97.48062	97.88826
“F1-Score”	96.32455	96.43463	96.38117	96.5269	98.25264
“MCC”	50.01494	49.89109	50.14905	50.00223	50.06145
For dataset 2					
“Accuracy”	89.47771	91.38021	91.84881	91.81629	96.28204
“Sensitivity”	92.25015	94.2901	94.78351	94.76199	97.88865
“Specificity”	96.33524	96.40741	96.43504	96.42055	98.25813
“Precision”	49.90867	49.98292	49.9186	50.05152	50.03937
“FPR”	7.749853	5.709897	5.216491	5.238008	2.111353
“FNR”	94.24707	95.33113	95.59695	95.5778	98.07241
“NPV”	89.47771	91.38021	91.84881	91.81629	96.28204
“FDR”	92.25015	94.2901	94.78351	94.76199	97.88865
“F1-Score”	96.33524	96.40741	96.43504	96.42055	98.25813
“MCC”	49.90867	49.98292	49.9186	50.05152	50.03937

Table 3. Performance validation on distinct heuristic strategies on proposed Deep Learning-based copy-move forgery identification scheme on dataset 2

Performance measures	SURF [34]	CNN [19]	RG2NN [35]	IFCSA-AT-RG2NN-FM
For dataset 1				
“Accuracy”	89.09751	91.54199	90.7167	94.36561

"Sensitivity"	91.84042	94.44415	93.58164	97.48062
"Specificity"	96.32455	96.43463	96.38117	96.5269
"Precision"	50.01494	49.89109	50.14905	50.00223
"FPR"	8.159575	5.555854	6.418364	2.519384
"FNR"	94.02612	95.42242	94.94901	97.00014
"NPV"	89.09751	91.54199	90.7167	94.36561
"FDR"	91.84042	94.44415	93.58164	97.48062
"F1-Score"	96.32455	96.43463	96.38117	96.5269
"MCC"	50.01494	49.89109	50.14905	50.00223
For dataset 2				
"Accuracy"	90.29179	89.8169	89.82467	96.65375
"Sensitivity"	93.12493	92.60627	92.6304	98.37912
"Specificity"	96.36403	96.35838	96.34161	98.16047
"Precision"	49.91589	49.96546	50.09372	52.16808
"FPR"	6.875067	7.393725	7.369596	1.620879
"FNR"	94.71481	94.4436	94.44665	98.26967
"NPV"	90.29179	89.8169	89.82467	96.65375
"FDR"	93.12493	92.60627	92.6304	98.37912
"F1-Score"	96.36403	96.35838	96.34161	98.16047
"MCC"	49.91589	49.96546	50.09372	52.16808

7. Conclusion

A new copy-move forgery identification model has been implemented to identify the forged images with a higher detection rate. Wanted images for identifying the copy-move forgeries were garnered from traditional online sources. The preprocessing techniques were applied over collected raw data and the deep as well as SURF features were extracted. Then, concatenation of both features was done and it was given to the AT-RG2NN-FM for identifying the matched key points between the images. Here, the descriptors match threshold has been optimally selected via the proposed IFCSA during feature matching from RG2NN. The matched key points have been helpful for the detection of forged images and the experimental outcome was compared with the previous algorithms and techniques to ensure the detection outcome. The comparison outcome were proved that the proposed model was attained with an improved detection accuracy of 7.04% than SURF, 7.61% than CNN, 7.60% than RG2NN for considering dataset 2 from Table 2. The forged images are effectively identified by using the proposed IFCSA-AT-RG2NN-FM-based copy-move forgery identification model when contrasted to the baseline approaches and heuristic strategies.

Acknowledgements

I would like to express my very great appreciation to the co-authors of this manuscript for their valuable and constructive suggestions during the planning and development of this research work.

Author Contribution

All authors have made substantial contributions to conception and design, revising the manuscript, and the final approval of the version to be published. Also, all authors agreed to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Conflict of Interest

The authors declare no conflict of interest

References

[1] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy–move forgery detection by matching triangles of key points," *IEEE Transactions on Information Forensics and Security*, Vol.10, pp. 2084-2094, 2015.

[2] A. Novozamsky, M. Sorel, "Detection of copy-move image modification using JPEG compression model",

Forensic Science International, Vol. 283, Pp. 47-57, 2018.

[3] Y. Wu, W. Abd-Almageed, and P. Natarajan, “Image Copy-Move Forgery Detection via an End-to-End Deep Neural Network”, *IEEE Winter Conference on Applications of Computer Vision*, 2018.

[4] J. Li, X. Li, B. Yang, and Xingming, “Segmentation-based Image Copy-move Forgery Detection Scheme”, *IEEE Transactions on Information Forensics and Security*, 2015.

[5] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, L. D. Tongo, G. Serra, “Copy-move forgery detection and localization by means of robust clustering with J-Linkage”, *Signal Processing: Image Communication*, Vol. 28, 2013.

[6] T. Mahmood, T. Nawaz, AunIrtaza, R. Ashraf, M. Shah, and M. Tariq Mahmood, “Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images”, *Mathematical Problems in Engineering*, 2016.

[7] F. Yanga, J. Lia, W. Lua, J. Wengb, “Copy-move forgery detection based on hybrid features", *Engineering Applications of Artificial Intelligence*, 2017.

[8] M. H. Alkawaz, G. Sulong, T. Saba and A. Rehman, "Detection of copy-move image forgery based on discrete cosine transform", *Natural Computing Applications*, 2016.

[9] D. Cozzolino, G. Poggi and L. Verdoliv, “Efficient dense-field copy-move forgery detection,” *IEEE Transactions on Information Forensics and Security*, Vol. 10, no. 11, pp.2284-2297, 2015.

[10] A. H. Oyiza, M. A. Maarof, “An improved DCT block-based technique for copy-move forgery detection in medical images”, *International Journal of Innovative Computing*, 2018.

[11] C. –S. Park, J. Y. Choeh, "Fast and robust copy-move forgery detection based on scale-space representation", *Multimedia Tools and Applications*, Vol.77, 2018.

[12] E. Silva, T. Carvalho, A. Ferreira, A. Rocha, “Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes", *Journal of Visual Communication and Image Representation*, Vol.29, Pp16-32, 2015.

[13] N. Kanagavalli and L. Latha, "A survey of copy-move image forgery detection techniques," International Conference on Inventive Systems and Control (ICISC), pp. 1-6,2017.

[14] I. Amerini, L. Ballan, R. Caldelli, Alberto Del Bimbo and Giuseppe Serra, “A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery”, *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 3, 2011.

[15] B. Yang, X. Sun, H. Guo, Z. Xia, X. Chen, "A copy-move forgery detection method based on CMFD-SIFT", *Multimedia Tools and Applications*, 2017.

[16] Y. Huang, W. Lu, W. Sun, D. Long, “Improved DCT-based detection of copy-move forgery in images”, *Forensic Science International*, Vol.206, Pp.178-184, 2011.

[17] O. M. Al-Qershi and B. E. Khoo, “Comparison of Matching Methods for Copy-Move Image Forgery Detection”, *Signal Processing and power applications*, 2017.

[18] S. Dhivya, J. Sangeetha, B. Sudhakar, “Copy-move forgery detection using SURF feature extraction and SVMsupervised learning technique”, *Soft Computing*, Vol. 24, 2020.

[19] B. Diallo, T. Urruty, P. Bourdon, C. Fernandez-Maloigne, ”Robust forgery detection for compressed images using CNN supervision”, *Digital Forensics*, 2020.

[20] Abhishek, N. Jindal, “Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation”, *Multimedia Tools and Applications*,2020.

[21] H. Chen, X. Yang, Y. Lyu, “Copy-Move Forgery Detection Based on Keypoint Clustering and Similar Neighborhood SearchAlgorithm”, *Digital Object Identifier*, 2020.

[22] Y. Zhu, C. Chen, G. Yan, Y. Guo, and Y. Dong,” AR-Net: Adaptive Attention and ResidualRefinement Network for Copy-MoveForgery Detection”, *IEEE Transactions on Industrial Informatics*, 2020.

[23] R. Agarwal, O. P. Verma, “An efficient copy move forgery detection using deep learning feature extraction and matching algorithm”, *Multimedia Tools and Applications*, 2019.

[24] M. A. Elaskily, H. A. Elnemr, A. Sedik, M. M. Dessouky, G. M. ElBanby, O. A. Elshakankiry, A. A. M. Khalaf, H. K. Aslan, O. S. Faragallah, F. E. A. El-Samie, ”A novel deep learning framework for copy-move forgery detection in images”, *Multimedia Tools and Applications*, 2020.

[25] B. Elhaminia, A. Harati, A. Taherinia, “A probabilistic framework for copy-move forgery detection based on Markov Random Field”, *Multimedia Tools and Applications*, 2019.

[26] J. Cardoso M. Santos, G. A. Carrijo, C. F. S. Cardoso, J. C. Ferreira, P. M. Sousa and A. C. Patrocínio, "Fundus image quality enhancement for blood vessel detection via a neural network using CLAHE and Wiener filter," *Research on Biomedical Engineering*, vol. 36, pp. 107–119, 2020.

[27] S. Firmansyah, and S. Anwar, "Perbaikan Citra Malam (Tidak Infrared) Dengan Metode Histogram Equalization Dan Contrast Stretching," *Jurnal Ilmu Pengetahuan Dan Teknologi Komputer*, Vol. 4. No. 2 February 2019.

[28] M. Zahid, F. Ahmed, N. Javaid, R. A. Abbasi, H. S. Z. Kazmi, A. Javaid, M. Bilal, M. Akbar and M. Ilahi, "Electricity Prices and Load Forecasting using Enhanced Convolutional Neural Network and Enhanced Support Vector Regression in Smart Grids," *Electronics*, vol. 8, pp. 122, 2019.

[29] S. Lu, X. Hu, C. Wang, L. Chen, S. Han, Y. Han, "Copy-move image forgery detection based on evolving circular domains coverage," *Multimedia Tools and Applications*, vol. 81, pp. 37847–37872, 2022.

[30] M. Ghaemi, and Mohammad-RezaFeizi-Derakhshi, "Forest Optimization Algorithm", *Expert Systems with Applications*, vol.41, no.15, pp.6676-6687, November 2014.

[31] A. S. Joshi, O. Kulkarni, G. M. Kakandikar, and V. M. Nandedkar, "Cuckoo Search Optimization- A Review", *Materials Today: Proceedings*, vol.4, no.8, pp.7262-7269, 2017.

[32] A. G. Gad, "Particle Swarm Optimization Algorithm and Its Applications: A Systematic Review," *Archives of Computational Methods in Engineering*, vol. 29, pp. 2531–2561, 2022.

[33] M. Jain, V. Singh, A. Rani, "A novel nature-inspired algorithm for optimization: Squirrel search algorithm," *Swarm and Evolutionary Computation*, Vol. 44, pp. 148-175, February 2019.

[34] F. Maher Al_azrak, Z. F. Elsharkawy, A. S. Elkorany, G. M. E. Banby, M. I. Dessowky & F. E. A. El-Samie, "Copy-Move Forgery Detection Based on Discrete and SURF Transforms," *Wireless Personal Communications*, vol. 110, pp. 503–530, 2020.

[35] S. Lu, X. Hu, C. Wang, L. Chen, S. Han, Y. Han, "Copy-move image forgery detection based on evolving circular domains coverage," *Multimedia Tools and Applications*, vol. 81, pp. 37847–37872, 2022.