Received: August 24, 2024. Revised: November 4, 2024.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Digital Image Forgery Detection Using Cyclic Symmetry Convolutional Neural Network

Shashikala S[1]* **Ravikumar G K[2]**

[1]*Department of Computer Science, New Horizon College, Kasturinagar, Bengaluru-43, Karnataka, India*
[2]*Department of Computer Science and Engineering, BGS College of Engineering and Technology, Mahalakshmipuram, Bengaluru-86, Karnataka, India*
* Corresponding author's Email: shashi127@yahoo.com

Abstract: Digital Image Forgery (DIF) detection involves identifying instances where a portion of image is copied and placed in different areas within same image to create a seemingly authentic but altered version. However, the detection of small duplicated regions is challenging, especially when noise is present in the image. This issue becomes more significant when the model is trained on noisy data as it negatively affects its accuracy. This research proposes an Elite Opposition-based Learning with Black Widow Spider Optimization (EBWSO) for feature selection and Cyclic Symmetry Convolutional Neural Network (CSCNN) for detection to enhance accuracy in image forgery detection. Pre-processing techniques such as Single Image Super-Resolution (SISR) and Histogram Equalization (HE) are used for image enhancement. The VGG16 and ResNet50 are used for feature extraction in digital images, done through identifying the key features such as edges and shapes. The EBWSO technique is utilized for feature selection by updating the relevant features and balancing exploration and exploitation. Detection is carried out using the CSCNN technique, which is designed to be rotation-invariant and aims to enhance detection accuracy. The EBWSO-CSCNN model accurately classifies image forgery when compared to the existing techniques such as Stacked Sparse Denoising Autoencoder (SSDAE) and Simple Linear Iterative Cluster (SLIC) algorithm. The proposed method achieves a better accuracy of 99.15% on MICC-F220, 98.10% on MICC-F600, 99.25% on MICC-F2000, and 98.95% on the CASIA 2.0 dataset.

Keywords: Black widow spider optimization, Cyclic symmetry convolutional neural network, Digital image forgery, Elite opposition-based learning, Simple linear iterative cluster.

1. Introduction

The widespread availability of digital image editing tools has raised serious concerns about image forgery and manipulation, impacting fields such as forensic investigation, journalism, and the preservation of digital archives [1]. Image forgery can be easily achieved using tools such as image editing software, PhotoPlus, etc. In the era of digitalization, images have become one of the most significant communication tools used in media and everyday life, making image forgery a prevalent issue [2]. The major approaches for detecting image forgery are divided into active and passive methods. The active approach involves inserting watermarks or digital signatures onto images during their creation, while the passive approach focuses on identifying changes that have altered correct information to incorrect information, or obscured important image details [3, 4]. However, continuous advancements in technology have led to the development of image tampering techniques that overcome traditional methods [5]. There are several post-processing operations such as rotation, resizing, and blending which can be used to modify images [6]. The most common models of image manipulation using deep learning techniques are copy-move and image splicing. These techniques involve replacing one or more fragments of an image with fragments from the same or various other images [7, 8].

A traditional detection method extracts particular image attributes including the image-compression characteristics, multiple objects, edge inconsistencies, and photo-response with no uniformity noise [9]. The explosion of digital images has led to the development of numerous image editing tools. In the digital era, several image processing techniques are used to improve image quality, aiding the pre-processing stage by focusing on image quality improvement [10]. Consequently, image forensics linked with digital image identification has become significant in network-based communities. The next phase is the feature extraction process which detects features in digital images such as edges, shapes, and motion. This improved identification allows for better data processing, facilitating various tasks related to image analysis [11, 12]. Counterfeiters also try to hide tampering effects by performing transformations, followed by parameter adjustments and noise addition before pasting the copied region. Optimization techniques update the current position to a new position by using feature selection to reduce dimensionality and enhance the opposition solution for efficient learning [13, 14]. Image forgery detection is challenging due to noise and poor image quality. Digital image forgery is classified into two categories: forgery and non-forgery using deep learning techniques [15]. However, recognizing very small duplicated areas in the image is challenging, and handling noise in the image can degrade performance if noise patterns in the training data affect accuracy. This research proposes an Elite Opposition-based Learning with Black Widow Spider Optimization (EBWSO) for feature selection and detection using a Cyclic Symmetry Convolutional Neural Network (CSCNN) to enhance accuracy in image forgery detection.

The main contributions of the research are shown below:

- Feature extraction is performed using pre-trained models like VGG16 and ResNet50 which effectively detect crucial features in digital images such as edges and shapes.
- The EBWSO technique optimizes feature selection by updating current location and opposite solution, enhancing model's ability to select relevant features and avoid local optima.
- The proposed EBWSO-CSCNN method significantly enhances detection accuracy, handles noise, and recognizes rotationally invariant features, leading to more robust image forgery detection.

The paper is organized as follows: Section 2 provides a literature review that summarizes digital image forgery detection by using DL, Section 3 introduces the proposed method utilized by CSCNN, while Section 4 discusses the result and comparative analysis, and Section 5 discusses the conclusion.

2. Literature review

This research conducts studies on digital image forgery (DIF), providing insights into various techniques along with their advantages and limitations.

Ye [16] presented a DIF detection method that involved copying and pasting regions of the original image. This method detected the tampered regions using deep learning techniques. The Simple Linear Iterative Cluster (SLIC) algorithm, without threshold was used in the super-pixel segmentation algorithm to obtain the tampering local region extraction algorithm using MICC-F220 & MICC-F2000 datasets. However, the performance of SLIC was highly dependent on chosen parameters such as the number of superpixels, noise in the image and the compactness factor.

Vijayalakshmi [17] introduced a DL-based technique using a Convolutional Autoencoder for DIF. This method manipulated the original contents of image using the MICC-F220 dataset. It reduced the dimensionality of data by learning a compressed encoding of the input and compressing data into a lower-dimensional space while retaining the essential information. The challenge with DIF in autoencoders was the difficulty in interpretation, making it inefficient to learn information and degrading the quality of reconstructed data, particularly if the autoencoder is not well-tuned, affecting accuracy in highly complex data.

Khalil [18] developed a deep neural network (DNN) for DIF using pre-trained models such as VGG19, ResNet50, MobileNetV2, Xception, and DenseNet on the CASIA 2.0 dataset. These models used residual connections to solve the vanishing gradient issue, enabling the training of deeper networks and efficient image classification due to their depth and effective learning capabilities. However, the pre-trained models limited the ability to learn features that distinguish authentic images from the manipulated ones when trained on large datasets.

Hammad [19] presented a conventional copy-move forgery detection (C-MFD) approach using AlexNet for deep learning and logistics techniques to extract features from images using the MICC-F600 & MICC-F2000 datasets. This approach was suitable for identifying and categorizing various objects within images and effectively detecting the high-level features. Nonetheless, AlexNet required

significant computational resources for training on large datasets, resulting in challenges in accuracy and high computational costs for image classification.

Gupta [20] introduced a DL-based Stacked Sparse Denoising Autoencoder (SSDAE) to classify image forgery and non-forgery using MICC-F2000, MICC-F220, MICC-FF600 & CASIA 2.0 datasets. The SSDAE, combined with Grasshopper Optimization Algorithm (GOA) and Spotted Hyena Optimizer (SHO), performed DIF detection with faster convergence rates and avoided local optima trapping. Nevertheless, recognizing very small duplicated areas in the image was challenging, and while denoising autoencoders were designed to handle noisy data, their performance was still degraded when noise patterns in training data affected accuracy.

Saleh Al Omari [21] presented a Doll Maker Optimization Algorithm (DOA) was derived from two natural behaviours in the doll making process. These was ability to exploration and exploitation them during the search process, which was help to avoid local optima and ensure more through coverage of solution space. However, DOA sensitive to choice of parameters such as population size, number of iterations and ability to explore diverse regions of the search space limited to algorithm.

Purba Daru Kusuma and Meta Kallista [22] developed a Migration-Crossover Algorithm (MCA) was single search evaluated to assess the essential of each search space. These was efficiently searching performed in third step by using of combination directed and crossover technique. However, unbalanced search space during neighbourhood search performed in 3 process it affects the accuracy.

Tareq Hamadneh [23] implemented an Addax Optimization Algorithm (AOA) was achieved effective solution for optimization approaches. These was high ability in exploration, exploitation and establishing a balances between search spaces. However, AOA approach struggle to maintain a balance between exploration and exploitation become excessive.

From the overall analysis, the existing techniques are seen to struggle with accurately detecting small, duplicated areas in the image, resulting in the performance often being degraded by noise, particularly when noise patterns in the training data affected the accuracy. Therefore, this research proposes EBWSO for feature selection and detection using a CSCNN to enhance accuracy in image forgery detection. This approach selects relevant and reduces high dimensionality, contributing to improving the classification accuracy.

3. Proposed methodology

In this section, EBWSO and CSCNN are used for image forgery detection to enhance accuracy. Initially, data is acquired from MICC-F220, MICC-F600, MICC-F2000, and CASIA 2.0 datasets. Pre-processing using SISR and HE is performed to enhance the image quality. Feature extraction using pre-trained models such as VGG-16 and ResNet 50 is performed to detect forged images and colourization from sources. The feature selection uses the optimization technique EBWSO to enhance the positions of the current and opposite solutions and to reach the global optimum. CSCNN is then used to classify and detect forged images and colourization from online sources. Fig. 1 illustrates block diagram of the proposed method.

3.1 Dataset

In this section, proposed EBWSO-CSCNN technique is calculated using MICCF-220, MICCF-600, MICCF-2000, and CASIA 2.0 benchmark datasets for classifying the digital image forgery.

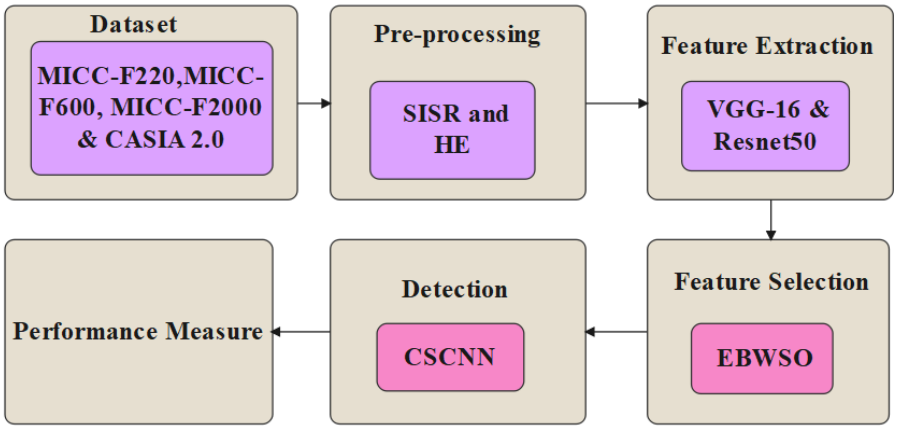

Figure. 1 Block diagram of proposed method

Table 1. represents the CASIA 2.0 dataset for digital image forgery

Number of image total	Authentic	Forged	Total	Size	Format
	7491	5123	12614	320x240x900x600	BMP, JPEG, TIFF

3.1.1. MICC-F220

The MICC-F220 [24] dataset consists of 220 images, evenly split between 110 tampered images and 110 original images. The dimensions of these images range between 722x480 to 800x600 pixels, with manipulated region comprising 1.2% of total image area.

3.1.2. MICC-F2000

The MICC-F2000 [25] dataset considers images 2000, consisting of 700 tampered images and 1300 original images. These high-resolution images measure 2048x1536 pixels, with manipulated regions comprising 1.12% of total image area.

3.1.3. MICC-F600

The MICC-F600 [26] dataset consists of 600 images, including 152 images with tampered regions and 448 original images. The dimensions of these images vary, ranging between 800x532 to 3888x2592 pixels. Notably, size of manipulated region various across images within this dataset.

3.1.4. CASIA 2.0

The CASIA 2.0 [27] dataset includes a total of 12,614 images, with 7,491 original images and 5,123 forged images, including 1,849 spliced images. These images are in JPEG and TIFF formats, with pixel dimensions ranging from 320x240 to 900x600. Table 1 provides a detailed description of the CASIA 2.0 dataset.

3.2 Pre-processing

After collecting data, pre-processing using Single Image Super-Resolution (SISR) and Histogram Equalization (HE) is employed for image enhancement and forgery detection [28]. These techniques maximum contrast between original and copied parts of an image. The enhancement assumption in forgery detection is that parts of the image are copied and edited. Motion cause pixel shifts, resulting in low-resolution images and missing information that high-resolution images provide. Image blurring and down-sampling degrade high-resolution images, but the SISR algorithm causes high-resolution images from minimized-resolution ones without external data. The goal of this technique is to increase image resolution, allowing the detection of small forgeries and improving the matching process. The pre-processed image is then used for feature extraction to detect features such as edges, shapes, and motion in digital images.

3.3 Feature extraction

After pre-processed data, feature extraction is carried out using ResNet-50 and VGG16 to extract image forgery. The ResNet-50-layer residual network's increased accuracy comes at the cost of higher computational resources. Training and inference with this model demand more memory and processing power. Due to its depth and complexity, ResNet-50 requires longer training time when compared to lightweight architectures [29]. In this research, it is necessary to consider this trade-off when choosing a model. Adapting deeper networks is advantageous for deep learning methods, and in this case, networks with 20-30 layers are utilized. The residual units allow training of a 152-layer model, where the extracted feature is 2046 for each image. There is a shallower learning curve due to the novel residual structure.

The VGG16 architecture involves taking weights and parameters learned from the existing VGG-16 model and applying DIF detection, wherein features include a max-pooling layer preceding a stack of 13 convolutional (Conv) layers and arrangements of Conv 16 model chosen for this study due to its sequential architecture. The extracted feature is used in 2096 for image forgery. Despite having more parameters and longer inference in forger, images are fine-tuned by adding layers and adjusting parameters based on model. The features extracted are given as input to feature selection to select relevant features involved in the DIF.

3.4 Feature selection

After feature extraction, feature selection using EOBL with BWSO referred to as the EBWSO method, selects relevant features for DIF detection. This process begins with the initial population of candidate solutions and generates opposition-based learning solutions by considering the opposite of each candidate solution. The EOBL enhances the exploration of search space, leading to selection of

more relevant features, while BWSO maintains diversity in population through crossover, mutation, and operations. This helps algorithm avoid getting stuck in local optima and increases the chances of finding the global optimum. This optimization technique reduces dimensionality of feature space by focusing on relevant features, wherein 78 % of 4096 and 2048 selected 3194 & 1597 features are taken in for forgery detection. The proposed algorithm starts with an initial population of spiders, where each spider represents a candidate solution.

3.4.1. Initial population

To optimize, each widow spider is assigned an appropriate structure for the solution, where position values of every black widow spider represent variables. The dimensional optimization is denoted as M_{var} with widow's array being $1 \times M_{var}$, as expressed in Eq. (1).

$$Widow = \left[z_1, z_2, \dots, z_{M_{var}}\right] \quad (1)$$

Where, $(z_1, z_2, \dots, z_{M_{var}})$ indicate variable values as assigned by floating point numbers, fitness of a widow is evaluated by fitness function, which is denoted as f at widow's position $(z_1, z_2, \dots, z_{M_{var}})$. The mathematical expression of fitness function is denoted by Eq. (2).

$$Fitness = f(widow) = f\left(z_1, z_2, \dots, z_{M_{var}}\right) \quad (2)$$

To begin optimization algorithm, a candidate in widow matrix of size $M_{pop} \times M_{var}$ is generated with an begin population of spiders. During procreation phase, male black widow is eaten by the female after mating.

3.4.2. Procreate

As the pairs are independent, they simultaneously begin mating to produce the next generation and each pair mates within its isolated web. Initially solitary, female and male spiders eventually unite for mating and reproduction. During mating, around 1000 eggs are produced, but only some spider eggs survive with the stronger ones prevailing. The algorithm reproduce and generate an array with random numbers containing offspring. Using Eq. (3), the offspring a_1 and a_1 are derived from the parents b_1 and b_2, as shown below.

$$\begin{cases} b_1 = \alpha \times a_1 + (1-\alpha) \times a_2 \\ b_2 = \alpha \times a_2 + (1-\alpha) \times a_1 \end{cases} \quad (3)$$

As long as the randomly chosen numbers are not duplicated, this process is repeated M_{var} 2 times. After being added to an array, the parents and kids are arranged according to their fitness values. The best people are added to the created population based on the cannibalism evaluations. The next stage is to couple each person.

3.4.3. Cannibalism

There are three kinds of cannibalism:

1. Male and female black widows eat each other during and after mating.
2. The female recognizes and eats the male based on their fitness function.
3. Baby spiders often eat their mother, with fitness values determining the strongest spiderlings

3.4.4. Movement

The black widow optimization considers movements within spider web in both linear and spiral fashion as represented in Eq. (4) & (5).

$$\vec{a}_i(t+1) = \vec{a}_*(t) - m\vec{a}_{r1}(t) \quad (4)$$

$$\vec{a}_i(t+1) = \vec{a}_*(t) - cos(2\pi\beta)\vec{a}_i(t) \quad (5)$$

Where, $\vec{a}_i(t+1)$ denotes separated position then improved in $\vec{a}_i(t)$ which denotes recent optimal separated position. The values are generated arbitrarily and fall within range of 0 to 1, with floating point values ranging from [0.4,0.9], when β ranges from [-1,1]. Integer values are assigned by r_1 and movement of black widow spider is determined by comparing the arbitrarily generated number to movement.

3.4.5. Sex pheromones

Sex pheromones play an essential role in behaviour of black widow spiders. Female black widows produce delay when they are well-fed compared to when they are starving. Male spiders are highly responsive to sex pheromones emitted by females, as these pheromones indicate a higher likelihood of fertility. By detecting these pheromones, male spiders avoid cost and risk associated with mating potentially hungry female spiders. The rate of pheromone production in black widow spiders is defined by Eq. (6).

$$pheromon\ (i) = \frac{fitness_{max} - fitness(i)}{fitness_{max} - fitness_{min}} \quad (6)$$

Where, the $fitness_{max}$& $fitness_{min}$ denote the best and worst of values in recent population and $fitness(i)$ solution of values in individual gender of i, respectively. The Pheromones vector contains a normalized fitness range is [0,1]. The updated position to individual gender is assigned in Eq. (7).

$$\vec{a}_i(t+1) = \vec{a}_*(t) + \frac{1}{2}[\vec{a}_{r1}(t) - (-1)^{\sigma}\vec{a}_{r2}(t)] \quad (7)$$

Where, $\vec{a}_i(t)$ denotes the place of female black widow spiders with minimum pheromone levels considered being $r1\,\&\,r2$ with arbitrary integers from one to zero population size and $r1 \neq r2$. The σ denotes the arbitrarily binary numbers of the range.

3.4.6. Mutation

In this stage, an arbitrarily selected number of individuals from the population undergo mutation. Each chosen solution arbitrarily exchanges 2 elements in the array. The mutation rate determines the mute pop. The stop conditions for the algorithm include a predefined number of iterations, which does not change in the fitness values over several consecutive iteration and reaches a specified level of accuracy. The BWSO method iteratively explores the solution until either desired level of accuracy is reached, or high amount of iterations is completed, aiming to identify the optimal outcome.

3.4.7. Proposed Elite Opposition-based Learning with Black Widow Spider Optimization

The algorithm search range and capabilities are increased by the EOBL technique, which is combined with BWSO to calculate both the current solution and opposite solution. The best people are chosen for population of the future generation by combining opposite population with current population through use of opposition-based learning technique. By doing this, likelihood of algorithm reaching a local optimum is decreased. The algorithm's convergence speed is accelerated by elite individuals' search data in current EOBL population, denoted as $a_n(h)$ and $a_n^*(h)$ for the opposition solution's generation h. The $a_{n,m}(h)$ and $a_{n,m}^*(h)$ are values on dimension m of $a_n(h)$ and $a_n^*(h)$, repectively. $e(2 \leq e \leq G)$ elite individuals are denoted as: $\{r_1(h), r_2(h), \ldots\ldots, r_r(h)\} \subseteq \{u_1(h), u_2(h), \ldots\ldots, u_G(h)\}$, and then $a_{n,m}^*(h)$ is defined the Eq. (8).

$$a_{n,m}^*(h) = \lambda\big(d_m(h) + f_m(h)\big) - a_{n,m}(h) \quad (8)$$

Where, $a_m(h) = \min\left(e_{1,m}(h)\right), f_m(h) = \max(e_{1,m}(h), .., e_{e,m}(h)$. The λ denotes the arbitrarily number of (0,1). The set of the bound treatment is as follows: if $a_{n,m}^*(h) > f_m(h)$, then $a_{n,m}^*(h) = f_m(h); if\, a_{n,m}^*(h) < d_m(h)$, followed by $a_{n,m}^*(h) = a_m(h)$. It is also shown that balancing exploitation and exploration of features helps achieve better accuracy. The elite opposition technique is introduced into original BWOA denoted as EBWOA which is executed at end of every iteration and select feature is fed to detection for copy-move forgery.

3.5 Detection

The detection using CSCNN techniques efficiently handles the feature process, reducing computational and training time while achieving high accuracy in classifying images as authentic or forged. CSCNN's ability to recognize rotationally invariant features is a significant advantage. Cyclic symmetry ensures that a network is unaffected by rotations of input image. This is particularly beneficial for image forgery detection, where image orientation is a crucial factor. The CNN potentially struggles with rotated images, whereas CSCNN handles such variations effortlessly and focuses on cyclic symmetric features, reducing complexity and improving efficiency of detection process. CSCNN has higher accuracy in image forgery detection due to its ability to extract more relevant and invariant features and reduce risk of overfitting on training data. Adding cyclic symmetric Conv layer in strategic positions within network maximizes benefit of rotation invariance. Training data to enhance CNN model by using standard backpropagation techniques ensures that cyclic symmetric properties are learned effectively.

The CNN model detects and handles DIF by involving its primary operational layers and input filters, enhancing outcomes efficiently based on CNN techniques. The network is designed to maximize the accuracy of model by optimizing use of input image. The CNN layers are arranged in a specific sequence to function as a feature extraction system, utilizing filters of fixed sizes. These filters are arranged to cover regions of input with some overlap known as stride. The subsequent convolutional layer extracts feature from maps learned by earlier layer. The subsequent Conv layers extract features from maps, which are learned from earlier Conv layers. Batch normalization is commonly applied in CNNs to classify output images, addressing challenges such as

information changes across layers and vanishing gradient issue. This is mathematically represented by Eq. (9) to (12), as shown below.

$$\mu\rho \leftarrow \frac{1}{m}\sum_{t=1}^{m} I_t \tag{9}$$

$$\sigma_{\beta}^{2} \leftarrow \frac{1}{m}\sum_{t=1}^{m}(I_t - \mu_{\beta})^2 \tag{10}$$

$$\widehat{I_t} = \frac{I_t - E[I_t]}{\sqrt{\sigma_{\beta}^{2} + \epsilon}} \tag{11}$$

$$I_t^{o} = \gamma\widehat{I_t} + \tag{12}$$

Where, I_t represents the ith training sample and batch sample amount is denoted as m, the mini batch input data is indicated as $\beta = \{I_t \ldots\ldots m\}$. The symbols σ_{β} and μ_{β} represent standard deviation and mean ϵ denoted as a constant used to prevent division by zero while γ and β are the parameters. The CNN goal by involving different architecture and different layers combined with cyclic symmetric, classifying the forgery image.

The cyclic slicing and pooling aggregate predictions from different rotated copies of input are deployed in permutation-invariant pooling function. The pooling operation occurs after 1 or more dense layers, where feature maps lose their spatial structure and inverse rotation realigns the feature map. To adapt an existing network architecture to be equivariance, a slicing layer is introduced at the input and a pooling layer at the output. Applying rotational augmentations to the training data ensures that the model learns rotationally invariant features. The model is then trained using the prepared data, monitoring loss and accuracy to ensure proper convergence. The cyclic slicing operation is represented as $S(n) = [n, rn, r^2x, r^3x]^T$; in practice, the column vector indicates that the rotated feature maps are stacked across the batch dimension. The 2 layers are straightforwardly modified to make the existing network invariant by including a slicing layer at the input side and a pooling layer at the outcome side.

To formalize this operation, the first image's equivariance properties are considered for slicing operation S. When involved input by it performing rotationally rx , $S(n) = [n, rn, r^2x, r^3x]^T = \sigma S(x)$ is acquired, where the elements are moved backward along the batch dimension by cyclic permutation, indicated by the symbol σ. A row vector is produced by realigning feature maps corresponding to various paths and stacking them along feature dimension using stacking method $T(x) = [x_0, r^{-1}x_1, r^{-2}x_2, r^{-3}x_3]$. The Conv layer uses padding is a cyclic symmetric manner, though it has not been fully explored. This cyclic Conv padding allows convolutional kernel to perform cyclic translation, sliding twice horizontally to capture complete translational variation. There are discrete filter with size of $(2n+1)^2 (n \in \mathbb{Z})$ and stride of cyclical Conv layer denoted as s. The filter is represented $\mathcal{K}$ successively from left to right mapped image, sliding and part beyond the border padding analysed left to right of the image until filter reappears on left of the image. The 2cycle is assigned to horizontal direction while the image mapped to translate the direction horizontally is expressed by Eqs. (13) and (14).

$$h_{out} = \frac{h_{in} - f - 1 + 2p}{s} + 1 \tag{13}$$

$$w_{out} = \frac{2w_{in} - f - 1 + 2p}{s} + 1 \tag{14}$$

Where, the input size of the cyclic convolutional is represented as $(h_{in}, 2w_{in})$ and the output size is $(h_{out}, 2w_{out})$, as formulated in Eq. (13) and (14). This setup increases the number of produced feature maps by a factor of 2, balancing parameters for each layer, which is proportional to both the number of input feature maps and filters. Rotating filters on feature maps affects the model's parameters rather than the input activation. This approach enhances accuracy through the handling of rotation symmetric, enabling the model to perform inference on variable-sized input.

4. Experimental results

This research proposes EBWSO-CSCNN, which is simulated in a Python environment using a system with 16GB RAM, an Intel Core i7 processor, and Windows 10 as operating system. To estimate model's performance metrics of accuracy, precision, recall, and f1-score are utilized in Eq. (15) and (18).

$$Accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)} \tag{15}$$

$$Precision = \frac{TP}{(TP+FP)} \tag{16}$$

$$F1 - measure = 2 * \frac{(Precision * Recall)}{Precision + Recall} \tag{17}$$

$$Recall = \frac{TP}{TP+FN} \tag{18}$$

Where, $TP, FN, FP,$ and TN denote the True Positive, False Positive, True Negative, and False Negative values, respectively.

4.1 Performance analysis

In this section, proposed method involving feature selection and detection processes is evaluated using several performance metrics including Accuracy, Precision, F1-measure, and Recall for MICC-F200, MICC-F600, CASIA 2.0 and MICC-F220 datasets. The performance of feature selection process with dataset is represented in Table 2, which describes feature selection results. The performance of different detection with default features using four datasets is represented in Table 3, which describes detection results. The performance of EBWSO feature selection is evaluated based on accuracy, precision, F1-measure, and recall on MICC-F220 dataset, as described in Table 2. The existing methods using feature selection techniques such as Grey Wolf Optimizer (GWO), Particle Swarm Optimization (PSO), Whale Optimization Algorithm (WOA) and BWSO are also evaluated. The EBWSO method achieves a high accuracy of 99.90% on MICC-F220, accuracy of 99.64 % on MICC-F600, accuracy of 99.25% on MICC-F2200, and accuracy of 98.95% on CASIA 2.0 datasets. The feature selection technique EBWSO achieves a high accuracy of 99.90% as it extracts related features to easily detect attacks.

The performance of CSCNN detection is evaluated based on accuracy, precision, F1-measure, and recall on MICC-F220 dataset, as described in Table 3. The existing methods using detection techniques such as RNN, DNN, DCNN and CNN are also evaluated.

The CSCNN method achieves a high accuracy of 99.90% on MICC-F220, accuracy of 99.64 % on MICC-F600, accuracy of 99.25% on MICC-F2200, and accuracy of 98.95% on CASIA 2.0 datasets. The EBWSO technique attains a superior accuracy of 99.90% as it extracts related features to easily detect attacks. Table 3 describes detection based on datasets, and Fig. 2 illustrates performance analysis of MICC-F2000 detection and Fig. 3 displays the performance analysis of detection of CASIA 2.0. The CSCNN is used for detection to learn and identify forged images through rotational analysis, followed by DIF detection.

Table 2. Evaluation of feature selection using datasets

Datasets	Methods	Accuracy (%)	Recall (%)	F1-Measure (%)	Precision (%)
MICC-F220	PSO	95.45	95.29	95.15	97.85
	GWO	96.56	96.68	96.25	96.96
	WOA	97.69	97.45	97.45	97.15
	BWSO	98.89	98.65	98.99	98.45
	Proposed EBWSO – CSCNN method	**99.15**	**98.85**	**98.60**	**98.80**
MICC-F600	PSO	94.52	81.02	87.95	84.63
	GWO	95.45	82.42	88.26	85.03
	WOA	96.56	83.32	89.15	86.52
	BWSO	97.69	84.36	90.42	87.12
	Proposed EBWSO – CSCNN method	**98.10**	**85.28**	**91.50**	**88.51**
MICC-F2000	PSO	95.03	81.02	87.06	84.89
	GWO	96.12	82.78	88.48	85.56
	WOA	97.85	83.45	89.26	86.23
	BWSO	98.36	84.12	90.15	87.23
	Proposed EBWSO – CSCNN method	**99.25**	**85.30**	**91.59**	**88.50**
CASIA 2.0	PSO	94.27	93.08	93.59	92.14
	GWO	95.68	94.86	94.86	93.68
	WOA	96.37	95.73	95.26	94.37
	BWSO	97.34	96.15	96.15	95.04
	Proposed EBWSO – CSCNN method	**98.95**	**97.84**	**97.58**	**96.12**

Table 3. Performance analysis of the detection of the datasets

Datasets	Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-Measure (%)
MICC-F220	RNN	95.45	97.85	95.29	95.15
	DNN	96.56	96.96	96.68	96.25
	DCNN	97.69	97.15	97.45	97.45
	CNN	98.89	98.45	98.65	98.99
	Proposed EBWSO – CSCNN method	99.15	98.80	98.85	98.60
MICC-F600	RNN	94.52	84.63	81.02	87.95
	DNN	95.45	85.03	82.42	88.26
	DCNN	96.56	86.52	83.32	89.15
	CNN	97.69	87.12	84.36	90.42
	Proposed EBWSO – CSCNN method	98.10	88.51	85.28	91.50

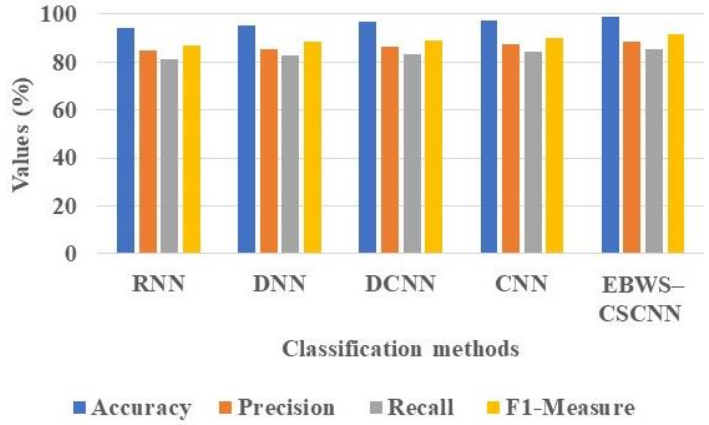

Figure. 2 Performance analysis of the detection of MICC-F2000

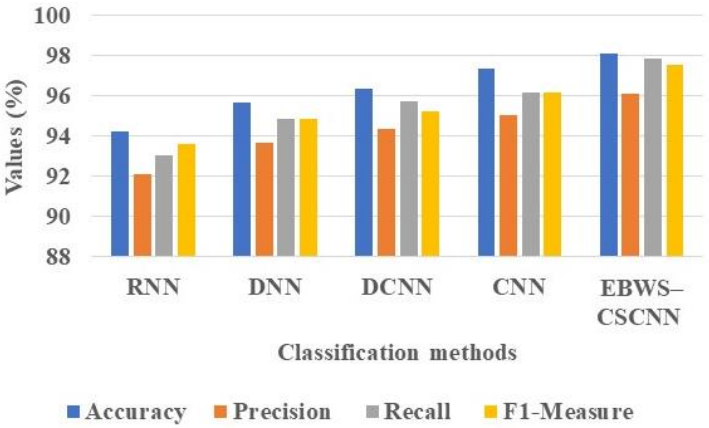

Figure. 3 Performance analysis of the detection on CASIA 2.0

4.2 Comparative analysis

The performance of the proposed EBWSO-CSCNN method achieves better accuracy when compared to the existing methods including SLIC [16], Autoencoder [17], VGG 19 [18], AlexNet [19] and SSDAE [20]. The comparative analysis involves 4 datasets: MICC-F200, CASIA 2.0, MICC-F220, and MICC-F600. In this research, proposed EBWSO-CSCNN method attainsa superior accuracies of 99.15% on MICC-F200, 98.10% on MICC-F600, 98.95% on MICC2000 and 98.11% on CASIA 2.0 dataset. Table 4 describes a comparative analysis of proposed method. Digital image forgery detection considers improved optimization combined with DL-based techniques, which further aids learn patterns efficiently with enhanced accuracy.

Table 4. Comparative analysis of the proposed method

Datasets	Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-Measure (%)
MICC-F220	SLIC [16]	N/A	N/A	N/A	95.09
	Autoencoder [17]	99.02	N/A	95.79	96.09
	SSDAE[20]	97.45	98.75	98.25	98.54
	Proposed EBWSO – CSCNN method	**99.15**	**98.80**	**98.85**	**98.60**
MICC-F600	AlexNet [19]	94.00	N/A	N/A	N/A
	SSDAE [20]	98.92	88.45	85.21	91.41
	Proposed EBWSO – CSCNN method	**98.10**	**88.51**	**85.28**	**91.50**
MICC-F2000	SLIC [16]	N/A	N/A	N/A	94.03
	AlexNet [19]	71.00	N/A	N/A	N/A
	SSDAE [20]	98.92	88.42	85.21	91.41
	Proposed EBWSO – CSCNN method	**99.25**	**91.50**	**90.30**	**92.59**
CASIA 2.0	VGG19 [18]	94.77	94.81	94.73	N/A
	SSDAE [20]	98.02	96.03	97.74	97.48
	Proposed EBWSO – CSCNN method	**98.95**	**97.12**	**98.84**	**98.58**

Table 5. Evaluated of proposed method on CASIA 2.0 dataset

Datasets	Methods	AUC
CASIA 2.0	VGG19 [18]	0.95
	Proposed EBWSO – CSCNN method	**0.96**

5. Discussion

This section discusses advantages of proposed model and analyses outcomes from EBWSO-CSCNN method. The proposed method is analysed on CASOA 2.0, MICC-F200, MICC-F220, and MICC-F600 datasets to efficiently classify forgery images. Initially, pre-processing using SISR and HE techniques is performed to enhance image quality. Feature extraction utilizes a pre-trained model efficient in extracting image edges and shapes, while feature selection using the EBWSO optimization enhances current position, avoids local optima, selects relevant features, and reduces dimensionality. The CSCNN technique enhances detection by dividing the image to efficiently distinguish between forgery and non-forgery images, thereby enhancing the accuracy. The proposed EBWSO-CSCNN method accomplishes a commendable accuracy rates of 99.15% on MICC-F220, 98.10% on MICC-F600, 98.11% on CASIA 2.0, and 98.95% on MICC-F200 datasets. The traditional methods of SLIC [16], Autoencoder [17], ResNet50 [18], AlexNet [19], and SSDAE [20] are also considered for comparison.

6. Conclusion

This research proposes an EBWSO-CSCNN method to enhance detection accuracy in image forgery detection. Pre-processing techniques such as SISR and HE are used for image enhancement and forgery detection. Feature extraction is performed using pre-trained models like VGG16 and ResNet50, which detect the features in digital images such as edges and shapes. The EBWSO technique updates the current position and opposite solution for feature selection, while detection using CSCNN technique is designed to be invariant to rotations, involving rotational manipulation and advanced accuracy. Finally, EBWSO-CSCNN model accurately classifies image forgery when compared to existing techniques, SSDAE and SLIC algorithms. The proposed method achieves high accuracy rates of 99.15% on MICC-F220, 99.25% on MICC-F600, 98.95% on MICC-F200, and 98.95% on the CASIA 2.0 datasets. Future work will consider hybrid techniques to evaluate detection based on various data classes.

Notation

Notation	Description
M_{var}, $1 \times M_{var}$,	Dimensional optimization with widow array
$(z_1, z_2, \ldots, z_{M_{var}})$	Variable values by floating and widow position
$M_{pop} \times M_{var}$	Size of widow matrix

a_1 and a_1, b_1 and b_2	Offspring from parents
$\vec{a}_i(t+1)$	Separated position
r_1	Integer values
$fitness_{max}$& $fitness_{min}$	Best and worst
[0,1]	Fitness range
$\vec{a}_i(t)$	Female black widow spiders
$r1$ & $r2$	Minimum pheromone levels
$a_n(h)$ and $a_n^*(h)$	Current EOBL population
$e(2 \le e \le G)$	Elite individual values
$a_m(h)$ $= \min\left(e_{1,m}(h)\right), f_m(h)$ $= \max(e_{1,m}(h),..,e_{e,m}(h).$	Maximum and minimum
I_t, m	Training sample and batch sample
$\beta = \{I_t \dots\dots m\}$	Input dat in CSCNN
γ and β	Constant parameter in CNN
$S(n) = [n, rn, r^2x, r^3x]^T$	Cyclic slicing operation
$(2n+1)^2 (n \in \mathbb{Z})$	Discrete filter
$\mathcal{K}$	Filter from left to right
$(h_{in}, 2w_{in})$ and $(h_{out}, 2w_{out})$,	Input size of cyclic convolutional and output size
$TP, FN, FP,$ and TN	True Positive, False Positive, True Negative, and False Negative values

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd author.

References

[1] M. S. Kaushik, and A. B. Kandali, "Hybrid Feature Selection for Effective Copy-Move Forgery Detection", *International Journal of Intelligent Engineering & Systems*, Vol. 17, No. 2, 2024, doi: 10.22266/ijies2024.0430.07.

[2] S.K. Narasimhamurthy, V. K. Mahadevachar, and R. K. T. Narasimhamurthy, "A Copy-Move Image Forgery Detection Using Modified SURF Features and AKAZE Detector", *International Journal of Intelligent Engineering & Systems*, Vol. 16, No. 4, pp. 12-24, 2023, doi: 10.22266/ijies2023.0831.02.

[3] K. M. Hosny, A. M. Mortda, M. M. Fouda and N. A. Lashin, "An Efficient CNN Model to Detect Copy-Move Image Forgery", *IEEE Access*, vol. 10, pp. 48622-48632, 2022, doi: 10.1109/ACCESS.2022.3172273.

[4] D. Patil, K. Patil, and V. Narawade, "A Novel Approach to Image Forgery Detection Techniques in Real World Applications," In: *Applications of Artificial Intelligence and Machine Learning: Select Proceedings of ICAAAIML 2021 Singapore: Springer Nature Singapore*, pp.461-473, 2022.

[5] J. Rao, S. Teerakanok and T. Uehara, "ResTran: Long Distance Relationship on Image Forgery Detection", *IEEE Access*, vol. 11, pp. 120492-120501, 2023.

[6] S. Krishnamurthy, K. A. Neelegowda, and B.G. Prasad, "IFLNET: Image Forgery Localization Using Dual Attention Network", *International Journal of Intelligent Engineering & Systems*, Vol. 15, No. 6, pp. 166-178, 2022, doi: 10.22266/ijies2022.1231.17.

[7] F.Z. El Biach, I. Iala, H. Laanaya, and K. Minaoui, "Encoder-decoder based convolutional neural networks for image forgery detection", *Multimedia Tools and Applications*, Vol. 81, pp.22611–22628, 2022.

[8] M.S. El Tokhy, "Development of precise forgery detection algorithms in digital radiography images using convolution neural network", *Applied Soft Computing*, 138, p.110174, 2023, doi: 10.1016/j.asoc.2023.110174.

[9] Z. Yang, B. Liu, X. Bi, B. Xiao, W. Li, G. Wang, and X. Gao, "D-Net: A dual-encoder network for image splicing forgery detection and localization", *Pattern Recognition*, Vol. 155, p.110727, 2024.

[10] S. Tyagi, and D. Yadav, "A detailed analysis of image and video forgery detection techniques", *The Visual Computer*, Vol. 39, pp.813-833, 2023.

[11] M. Maashi, H. Alamro, H. Mohsen, N. Negm, G. P. Mohammed, N. A. Ahmed, S.S. Ibrahim, and M. I. Alsaid, "Modeling of Reptile Search Algorithm With Deep Learning Approach for Copy Move Image Forgery Detection", *IEEE Access*, vol. 11, pp. 87297-87304, 2023.

[12] H. Ding, L. Chen, Q. Tao, Z. Fu, L. Dong, and X. Cui, "DCU-Net: a dual-channel U-shaped network for image splicing forgery

detection", *Neural Computing and Applications*, Vol. 35, pp.5015-5031, 2021.

[13] B. Fatima, A. Ghafoor, S.S. Ali, and M.M. Riaz, "FAST, BRIEF and SIFT based image copy-move forgery detection technique", *Multimedia Tools and Applications*, Vol. 81, pp.43805-43819, 2022.

[14] G. Tahaoglu, G. Ulutas, B. Ustubioglu, M. Ulutas, and V. V. Nabiyev, "Ciratefi based copy move forgery detection on digital images", *Multimedia Tools and Applications*, Vol. 81, pp. 22867-22902, 2022.

[15] M.M.A. Alhaidery, A.H. Taherinia, and H.I. Shahadi, "A robust detection and localization technique for copy-move forgery in digital images", *Journal of King Saud University-Computer and Information Sciences*, Vol. 35, No. 1, pp.449-461, 2023.

[16] W. Ye, Q. Zeng, Y. Peng, Y. Liu, and C.C. Chang, "A two-stage detection method of copy-move forgery based on parallel feature fusion", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2022, p.30, 2022.

[17] N.V.S.K. Vijayalakshmi, J. Sasikala, and C. Shanmuganathan, "Copy-paste forgery detection using deep learning with error level analysis", *Multimedia Tools and Applications*, Vol. 83, pp.3425-3449, 2024.

[18] A.H. Khalil, A.Z. Ghalwash, H.A.G. Elsayed, G.I. Salama, and H. A. Ghalwash, "Enhancing Digital Image Forgery Detection Using Transfer Learning", *IEEE Access*, Vol. 11, pp. 91583-91594, 2023.

[19] B.T. Hammad, I.T. Ahmed and N. Jamil, "An Secure and Effective Copy Move Detection Based on Pretrained Model", In: *Proc. of 2022 IEEE 13th Control and System Graduate Research Colloquium (ICSGRC)*, Shah Alam, Malaysia, Vol. 2022, pp. 66-70, 2022.

[20] R. Gupta, P. Singh, T. Alam, and S. Agarwal, "A deep neural network with hybrid spotted hyena optimizer and grasshopper optimization algorithm for copy move forgery detection", *Multimedia Tools and Applications*, Vol. 82, pp.24547-24572, 2022.

[21] K. Kaabneh, I. AbuFalahah, K. Eguchi, S. Gochhait, I. Leonova, Z. Montazeri, and M. Dehghani, "Dollmaker Optimization Algorithm: A Novel Human-Inspired Optimizer for Solving Optimization Problems", *International Journal of Intelligent Engineering & Systems*, Vol. 17, No. 3, pp. 816-828, 2024, doi: 10.22266/ijies2024.0630.63.

[22] P. D. Kusuma, and M. Kallista, "Migration-Crossover Algorithm: A Swarm-based Metaheuristic Enriched with Crossover Technique and Unbalanced Neighbourhood Search", *International Journal of Intelligent Engineering & Systems*, Vol. 17, No. 1, pp. 698-710, 2024, doi: 10.22266/ijies2024.0229.59.

[23] T. Hamadneh, K. Kaabneh, O. Alssayed, K. Eguchi, S. Gochhait, I. Leonova, and M. Dehghani, "Addax Optimization Algorithm: A Novel Nature-Inspired Optimizer for Solving Engineering Applications", *International Journal of Intelligent Engineering & Systems*, Vol. 17, No. 3, pp. 732-743, 2024, doi: 10.22266/ijies2024.0630.57.

[24] MICC-F220 dataset: https://www.kaggle.com/datasets/mashraffarouk/micc-f220 (Accessed on July 2024).

[25] MICC-F600 dataset: https://www.kaggle.com/datasets/nishaahin/miccf600 (Accessed on July 2024).

[26] MICC-F2000 dataset: https://www.kaggle.com/datasets/manas29/micc-f2000 (Accessed on July 2024).

[27] CASIA 2.0 dataset: https://www.kaggle.com/datasets/divg07/casia-20-image-tampering-detection-dataset (Accessed on 2024).

[28] A. Baumy, A.D. Algarni, M. Abdalla, W. El-Shafai, F. E. A. El-Samie, and N. F. Soliman, "Efficient Forgery Detection Approaches for Digital Color Images," *Computers, Materials & Continua*, Vol. 71, No.2, pp. 3257-3276, 2022.

[29] A. Arini, R. Broer Bahaweres and J. Al Haq, "Quick Classification of Xception And Resnet-50 Models on Deepfake Video Using Local Binary Pattern", In: *Proc. of 2021 International Seminar on Machine Learning, Optimization, and Data Science (ISMODE)*, Jakarta, Indonesia, pp. 254-259, 2022.