BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **22**, No 4
Sofia • 2022 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2022-0041

Copy-Move Forgery Detection Using Superpixel Clustering Algorithm and Enhanced GWO Based AlexNet Model

Sreenivasu Tinnathi[1*], *G. Sudhavani*[2]

[1]*Department of ECE, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India*
[2]*Department of ECE, R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India*
E-mails: sreenivasut@outlook.com / sreenivasut@srivasaviengg.ac.in gsudhavani@rvrjc.ac.in

***Abstract*:** *In this work a model is introduced to improve forgery detection on the basis of superpixel clustering algorithm and enhanced Grey Wolf Optimizer* (*GWO*) *based AlexNet. After collecting the images from MICC-F600, MICC-F2000 and GRIP datasets, patch segmentation is accomplished using a superpixel clustering algorithm. Then, feature extraction is performed on the segmented images to extract deep learning features using an enhanced GWO based AlexNet model for better forgery detection. In the enhanced GWO technique, multi-objective functions are used for selecting the optimal hyper-parameters of AlexNet. Based on the obtained features, the adaptive matching algorithm is used for locating the forged regions in the tampered images. Simulation outcome showed that the proposed model is effective under the conditions: salt & pepper noise, Gaussian noise, rotation, blurring and enhancement. The enhanced GWO based AlexNet model attained maximum detection accuracy of 99.66%, 99.75%, and 98.48% on MICC-F600, MICC-F2000 and GRIP datasets.*

***Keywords*:** *Adaptive Matching Algorithm, AlexNet, Copy-Move Forgery Detection, Grey Wolf Optimizer, Superpixel Clustering Algorithm.*

1. Introduction

In recent decades, abundant multimedia images are generated, due to the rapid growth of internet technology [1, 2]. The multimedia images are used in numerous research fields like media misinformation, social media, intelligence, military operations, newspapers, defamation of famous characters, evidence in courts and many other applications [3-5]. The image editing tools like paint shop Pro and Adobe Photoshop are used to modify the content and appearance of images without leaving perceptible artifacts [6]. Numerous authentication techniques are introduced to secure the image communication process, where the authentication techniques are categorized into two types: active and passive authentication. Active authentication includes the techniques like cryptography, watermarking, etc., and inactive authentication, the original image content is available and compared with the test image, where the original image content is unavailable in passive authentication [7]. The test image is

investigated without prior knowledge of the original image content, where this type of authentication is applied in forgery detection [8-10]. Compared to other image forgeries like re-touching and splicing, copy-move is the wide-spread image forgery, due to its easy implementation and hard nature in recognition [11, 12]. The limited effects on digital images make copy-move forgery detection a challenging task [13]. Further, the forged regions have similar characteristics and features to the original host image, so most of the existing keypoint-based forgery recognition techniques fail to achieve better detection accuracy [14]. To highlight the aforementioned issues, an efficient and reliable recognition model is proposed in this paper. The contributions of this work are listed as follows.

- Superpixel Clustering Algorithm is applied to segment the patches in the images, which are collected from the datasets like MICC-F600, MICC-F2000 and GRIP.
- A Deep Learning Based Feature Extraction is performed using an enhanced GWO based alexNet model to extract feature vectors from the dissimilar scales of segmented patches. Enhanced GWO technique utilizes two multi-objective functions: leader selection strategy and Pareto archive for optimal hyper-parameter selection that improves the converge rate and reduces the running time of the model.
- The Adaptive Matching Algorithm is used to extract similar keypoints in every patch for forgery localization. The proposed model performance is examined using the performance measures: recall, accuracy, precision, F-score, Prevalence Threshold (PT), error rate, False Omission Rate (FOR), and False Discovery Rate (FDR).

This paper is organized as follows: some existing papers on the topic "copy-move forgery detection" are surveyed in Section 2. The theoretical explanation and experimental analysis of the proposed enhanced GWO based AlexNet model are represented in Sections 3 and 4. Lastly, the conclusion of this study is depicted in Section 5.

2. Related works

Tinnathi and Sudhavani [15] used an adaptive watershed segmentation algorithm for partitioning the forged image into the non-overlapped segments. To improve the segmentation performance and to remove the undesired regional minima, an adaptive galactic swarm optimizer was applied for selecting the optimal parameters. Further, hybrid wavelet Hadamard transform and random sample consensus technique were applied for feature extraction and optimal feature selection. Finally, the forgery region extraction method was presented to recognize the copied regions in the host images, where the implemented model was computationally complex. Kasban and Nassar [16] firstly transforms the RGB image into YCbCr space and further, Hilbert huang transform was used for extracting feature values from the chrominance red-component Cr. Next, classification was performed utilizing different techniques in that Support Vector Machine (SVM) achieved higher detection accuracy in forgery detection, but it supports only binary classification. Elaskily et al. [17] developed a novel Convolutional Neural Network (CNN) for

copy-move forgery detection. The CNN model learns hierarchical features from the collected images having been used to detect the forged regions. Meena and Tyagi [18] initially categorized the original images into over-lapping blocks, and further, 12 high pass and 4 low pass coefficients were extracted from each over-lapping block using Tetrolet transform. Lexicographically, the extracted feature vectors were sorted, and then the similar blocks were determined for matching the extracted Tetrolet feature vectors. The CNN model requires a larger amount of data for achieving better classification results. Agarwal and Verma [19] utilized the Simple Linear Iterative Clustering (SLIC) Algorithm and VGGNet model to segment tampered patches and to extract feature values from the segmented tampered patches. An adaptive patch matching method was used to identify the suspicious regions and then the segmented tampered patches were matched with the suspicious regions for classifying both forged and unforged regions. Zhu et al. [20] presented an end-to-end neutral network based on residual refinement network and adaptive attention for copy-move forgery detection. Here, the channel and position attention feature vectors were combined using the adaptive attention process to enrich the feature representation and to capture the context information. Then, the matching process was accomplished by atrous spatial pyramid pooling for generating the coarse masks. Next, the coarse masks were optimized by residual refinement that helps in retaining the structures of object boundaries. Liu, Guan and Zhao [21] developed a convolutional kernel model for copy-move forgery detection. The deep learning models: VGGNet, residual refinement network and convolutional kernel were computationally costly.

Lin et al. [22] used Scale-Invariant Feature Transform (SIFT) and Local Intensity Order Pattern (LIOP) descriptors to extract features from the original image. Further, the matching relationship was improved by using transitive matching and the false matches were removed using the filtering approach. Lastly, the affine transformation was used to locate the duplicated regions in the images. Alberry, Hegazy and Salama [23] combined fuzzy C means algorithm and SIFT for effective copy-move forgery detection. Yang et al. [24] used SIFT and KAZE feature descriptors to extract feature vectors/points from the original images. Then, an improved matching technique was used to identify the best matched feature points. Further, a filtering technique and an iteration strategy were used to eliminate the false matches, and finally, the correlation coefficient map was utilized for locating the duplicate regions. However, the SIFT descriptor was computationally heavy and mathematically complicated. Niyishaka and Bhagvati [25] used Binary Robust Invariant Scalable Keypoints (BRISK) descriptor and image blob for finding similar keypoints in the original image for an effective copy-move region detection. Huang and Ciou [26] used a SIFT descriptor to extract important key-points from the original images. Further, the Helmert transformation technique was applied to group the matching pairs to obtain the coarse forgery regions. Finally, the isolated areas were eliminated from the coarse forgery regions for locating the forgery regions more accurately. The simulation results showed that the use of hand-crafted features like BRISK and SIFT obtained only comparable performance under the conditions of the post-processing operations (jpeg compression, image blurring and noise addition)

and geometric transformations (rotation and scaling). Wang et al. [27] developed super-pixel segmentation to divide the images into non-overlapping blocks and further, feature extraction was carried out by polar complex exponential transform and Speeded-Up Robust Feature (SURF) descriptor. The dense matched feature points were identified by eliminating the false matched points for achieving effective copy-move forgery detection, but the developed model was computationally complex.

Raju and Nair [28] developed a binary discriminative feature descriptor to detect suspected regions in the original images. The presented model obtained comparable forgery detection performance under the conditions such as brightness change, color blurring, color reduction, and contrast adjustments. Gani and Qadir [29] used discrete cosine transform technique for extracting feature vectors from the original images. In addition, kd-tree based nearest neighbor searching technique was used for matching the extracted feature vectors to identify the duplicate regions in the images. Soni, Das and Thounaojam [30] developed a SURF descriptor for extracting feature values from the original images. Next, two nearest neighbor and affine transform were applied to match the extracted feature vectors for better forgery detection. However, the discrete cosine transform technique and SURF descriptor were computationally intensive. Chen, Lu and Chou [31] employed region growing strategies and SIFT descriptor for rotational copy-move forgery detection. In addition, Park et al. [32] combined local binary patterns and SIFT descriptors for detecting copy-move forgeries in the images. The semantic space between the extracted feature subsets was high, while utilizing the hand-crafted feature vectors that may reduce the classification results. Elhaminia, Harati and Taherinia [33] utilized a probabilistic system on the basis of Markov random field to detect copy-move forgeries on the MICC-F220 and MICC-F600 datasets. Bilal et al. [34] used SURF descriptor and spatial clustering algorithm to extract features and to match the similar features for the detection of copy-move forgery regions. As stated earlier, the hand-crafted features like SURF were not robust and computationally intensive, due to high dimensions. Chen et al. [35] used Fractional Quaternion Zernike Moments (FrQZMs) and modified patch matching algorithm for both feature extraction and matching. However, the traditional models, especially keypoint based methods fail in handling the cases, while copy-move forgeries only involve smooth and small regions. Further, the keypoint based methods fail to classify the naturally identical regions and copy-move regions.

The motivation of this research manuscript is to propose a new model for image forgery recognition. The proposed enhanced GWO based AlexNet model has the capability in detecting small tampering regions and achieving high detection accuracy against image manipulation attacks such as salt & pepper, Gaussian noise, rotation, blurring and enhancement. A detailed explanation of the proposed model: Enhanced GWO Based AlexNet model is given in Section 3.

3. Methodology

In copy-move forgery detection, the proposed model consists of four steps: data collection: MICC-F600, MICC-F2000 and GRIP dataset, patch segmentation: superpixel clustering, feature extraction: Enhanced GWO based AlexNet model, and forgery localization: Adaptive matching algorithm, which are briefly detailed below.

3.1. Dataset description

In this work, the proposed enhanced GWO based AlexNet model performance is investigated on MICC-F600, MICC-F2000, and GRIP datasets. The GRIP dataset comprises 80 images with a pixel resolution of 768×1024 [36]. In the GRIP dataset, the forged regions in the original images are of different shapes and sizes that making forgery detection challenging. The link to download the GRIP dataset is http://www.grip.unina.it/. Similarly, the MICC-F600 dataset comprises 600 images (440 original images and 160 tampered images) with pixel resolution ranges between 800×532 and 3888×2592 [37]. In the MICC-F600 dataset, the size of the tampered region varies from one image to another image. Further, the MICC-F2000 dataset consists of 2000 images (1300 original images and 700 tampered images) with a pixel resolution of 2048×1536. In the MICC-F2000 dataset, the tampered regions indicate 1.12% of the whole original images. The link to download MICC-F600 and MICC-F2000 datasets is **http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/**.

3.2. Patch segmentation

After the collection of tampered images, the patch segmentation process is performed using the superpixel clustering algorithm that works based on k-means clustering. The superpixel clustering algorithm segments the similar pixels from the tampered images, which are technically named superpixels. Initially, the collected tampered images are fed to the CIELAB that contains two vectors: pixel position and color value of the pixels [38]. The position P and color value cv of the pixels are mathematically depicted in the next equations:

$$P = (x, y), \tag{1}$$

$$\mathrm{cv} = (l, a, b), \tag{2}$$

where $(x,\ y)$ represents image coordinates, and l, a and b denotes RGB color values. Further, the similarity between the feature vectors are estimated and then local clustering is used to segment the superpixels. In this clustering algorithm, the superpixel size is calculated by dividing the total pixels by separated superpixels. The Superpixel Size is mathematically depicted in the next equation:

$$\mathrm{SSp} = \sqrt{\frac{n}{\mathrm{Sp}}}, \tag{3}$$

where Sp indicates separated superpixels, and n denotes the number of pixels. The seed points in the image need to be moved towards 3×3 centered region during the clustering process, or else it leads to interference. By using the adjacent and own seed points, the similarity between the image pixels are calculated. The color difference and space distance between the image pixels is determined using the next equations:

(4) $$\mathrm{Dif}_{\mathrm{lab}} = \sqrt{(l_{\mathrm{Sp}} - l_i)^2 + (a_{\mathrm{Sp}} - a_i)^2 + (b_{\mathrm{Sp}} - b_i)^2},$$

(5) $$\mathrm{Dis}_{xy} = \sqrt{(x_{\mathrm{Sp}} - x_i)^2 + (y_{\mathrm{Sp}} - y_i)^2},$$

where, i denotes corresponding image pixels, and the pixel similarity is calculated using

(6) $$D_i = \mathrm{Dif}_{\mathrm{lab}} + \frac{m}{S}\mathrm{Dis}_{xy},$$

where, $m = \sqrt{(\mathrm{Spt1} - \mathrm{Spt2})\text{^}2}$, and $S = \frac{\mathrm{cv1}-\mathrm{cv2}}{255}$. The parameters m and S represent the distance, and color similarity between two seed points Spt1 and Spt2. The two-pixel values are similar, if the value of D_i is higher. As the result, more superpixels are segmented from the collected tampered image. In this scenario, the cluster size is fixed as 485, and the resultant image of the superpixel clustering algorithm is depicted in Fig. 1.

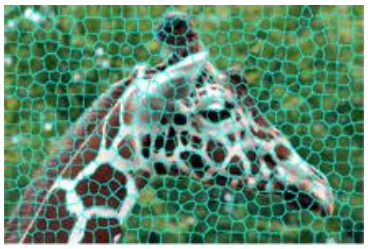


Fig. 1. Resultant image of Superpixel Clustering Algorithm

3.3. Feature extraction

After patch segmentation, feature extraction is performed using an enhanced GWO based AlexNet model to extract feature vectors from the dissimilar scales of segmented patches. In this paper, the enhanced GWO technique is combined with AlexNet model to select the optimal hyper-parameters that significantly diminish the model's running time, and improve the converge rate. As per the network requirements, the segmented images are resized to 227 × 227 pixels, which are given to the AlexNet model (pre-trained CNN) via the input layer for feature extraction [39]. The AlexNet model comprises eight layers like five convolutions and three fully connected layers, where each layer is followed by Rectifier Linear Unit (ReLU) activation function and max-pooling operation. Here, the feature vectors are extracted from the last fully connected layer with the help of softmax classifier. The extracted deep learning feature vectors have more detailed information and minor variations between the tampered and original region. In-depth reconstruction, the extracted feature vectors provide continuous matching pixels for identifying the tampered regions accurately. The hyper-parameters of the AlexNet model selected by enhanced GWO technique are momentum is 0.6, training algorithm is stochastic gradient descent, the learning rate is 0.015, validation frequency is 30, a maximum epoch is 10, and L2 regularization is 1.0000×10^{-4}. The design statistics of AlexNet model is depicted in Table 1.

Table 1. Design statistics of AlexNet model

Hidden layers	No	Design
Convolution	1	250 filters in size 5 × 5 with max pooling operation
	2	250 filters in size 3 × 3 with max pooling operation
	3	380 filters in size 3 × 3 with max pooling operation
	4	380 filters in size 3 × 3 with max pooling operation
	5	250 filters in size 3 × 3 with max pooling operation
Fully connected	1	3096 nodes with ReLU activation function
	2	3096 nodes with ReLU activation function
	3	200 nodes with ReLU activation function

The GWO is a swarm intelligence based technique, which is more reliable in hyper parameter optimization compared to other traditional optimization techniques [40]. Generally, the grey wolf belongs to the Canidae family, where a predominance gathering is maintained. Based on the leadership hierarchy, the grey wolves split into four groups such as alpha α, beta β, delta δ, and gamma γ. In this optimization technique, the decision making is done by the grey wolves belonging to the group α, where the grey wolves belongs to the group β are sub-ordinates, which assists in decision making. The third best solution and the remainder of the upcoming solution are considered as δ and γ. The GWO technique majorly includes three steps such as searching the prey, encircling, and attacking the prey. The traditional GWO technique uses simple principles for ranking the solutions in every iteration and updating their position [41]. In the enhanced GWO technique, multi-objective functions like leader selection strategy and Pareto archive are applied to select the best solutions, and to eliminate the crowded segments. In the GWO technique, the encircling process is mathematically indicated in the next equations:

$$\mathrm{dis} = \left|c \times z_{u(t)} - z(t)\right|, \tag{7}$$

$$z(t+1) = z_{u(t)} - k \times \mathrm{dis}, \tag{8}$$

where dis represents distance, t states present iteration, $z_{u(t)}$ indicates location of prey, $z(t)$ states position of grey wolf, k and c indicates coefficients. The coefficients $k = 2or_1 - o$ and $c = 2r_2$, where o is a decreasing parameter, r_1 and r_2 are random values that range between zero to one. In this technique, the grey wolves belong to α, β and δ know the prey's location to simulate hunting behaviour, which is mathematically depicted in the next equations:

$$\overrightarrow{\mathrm{dis}}_\alpha = |\vec{c}_1 \times \vec{z}_\alpha - \vec{z}|, \overrightarrow{\mathrm{dis}}_\beta = \left|\vec{c}_2 \times \vec{z}_\beta - \vec{z}\right| \text{ and } \overrightarrow{\mathrm{dis}}_\delta = |\vec{c}_3 \times \vec{z}_\delta - \vec{z}|, \tag{9}$$

$$\vec{z}(t) = \frac{\vec{z}_1 + \vec{z}_2 + \vec{z}_3}{3}, \tag{10}$$

where $\vec{z}_1 = \vec{z}_\alpha - \vec{k}_1 \times (\overrightarrow{\mathrm{dis}}_\alpha)$, $\vec{z}_2 = \vec{z}_\beta - \vec{k}_2 \times \left(\overrightarrow{\mathrm{dis}}_\beta\right)$, and $\vec{z}_3 = \vec{z}_\delta - \vec{k}_3 \times \left(\overrightarrow{\mathrm{dis}}_\delta\right)$.

Every cycle of the GWO technique generates new solutions, where the Pareto archive stores the non-dominated Pareto optimal solutions. An archive controller is used to control the archive that finds the non-dominated solutions for 30 iterations. Pareto archive eliminates the most crowded segments, if the number of non-dominated Pareto optimal solutions exceeds the archive size. In addition, the leader selection strategy selects α, β and δ using a roulette wheel of the least crowded segments that further saves the best non-dominated optimal solutions. The parameters used in enhanced GWO technique are; dimension is 4, number of agents is 30, batch

size is 32, iteration is 30, upper bounds is [1, 0.5, 15, 5.0000×10^{-4}], and lower bound is [0.5, 0.01, 5, 1.0000×10^{-4}]. The selected 320 AlexNet feature vectors are used for dense path re-construction.

3.4. Forgery localization

To identify the tampered region, the dense depth of the patches is re-constructed and matched with other patches. The suspicious tampered regions in the images are identified by comparing the patches. The key-point locations are re-localized to achieve effective re-construction with AlexNet feature vectors. Based on the re-located feature vectors, the Depth Map (DM) is generated to initialize the reconstruction process, which is mathematically defined in the equation

$$\mathrm{DM} = \{F_{i,j} | i \in 1, \ldots, w,\ j \in 1, \ldots, h\}, \tag{11}$$

where w indicates width of feature vector, h denotes height of feature vector, $F_{i,j}$ indicates color value or pixel brightness extracted as feature vectors at location i and j. The pixels depth (i, j) are calculated based on $\Delta\mathrm{DM} = 0$, as specified in the equation

$$4\mathrm{DM}_{i,j} - \mathrm{DM}_{i+1,j} - \mathrm{DM}_{i-1,j} - \mathrm{DM}_{i,j+1} - \mathrm{DM}_{i,j-1} = 0. \tag{12}$$

Further, the median difference dif_{xy} is determined on all the patches using the extracted feature vectors in order to re-construct the dense depth of the tampered image, and then dif_{xy} is compared with the median thresholding value th. Then, a new median difference $N\mathrm{dif}_{xy}$ is estimated, if the difference rate is lower than the th, which is mathematically stated in the equation

$$N\mathrm{dif}_{xy} = |In_x - In_y|, \tag{13}$$

where $\mathrm{In}_x - \mathrm{In}_y$ indicates patch Intensity. Then, each patch is transformed into binary value that helps in finding the tampered regions more efficiently and accurately. The re-construction of depth value diminishes the dissimilarity between the forged and original patches. The binary conversion is mathematically defined in equation

$$N\mathrm{dif}'(i,j) = \begin{cases} 0 & N\mathrm{dif}_{xy} \leq \mathrm{th} \\ 1 & N\mathrm{dif}_{xy} > \mathrm{th} \end{cases}. \tag{14}$$

Then, the similar keypoints are extracted in each patch using adaptive patch matching algorithm. The re-constructed patches are indicated as $\mathrm{RP} = \{\mathrm{RP}^1, \mathrm{RP}^2, \mathrm{RP}^3, \ldots, \mathrm{RP}^n\}$, where n denotes number of scales. Next, the correlation between the patches is calculated by matching the keypoints of the patches $\mathrm{CRP} = \{\mathrm{CRP}^1, \mathrm{CRP}^2, \mathrm{CRP}^3, \ldots, \mathrm{CRP}^n\}$, where CRP indicates Correlation Coefficients of the Patches. Further, the threshold value is calculated for each patch based on CRP, which is given as $\mathrm{th}_{\mathrm{RP}} = \{\mathrm{th}^1_{\mathrm{RP}}, \mathrm{th}^2_{\mathrm{RP}}, \mathrm{th}^3_{\mathrm{RP}}, \ldots, \mathrm{th}^{\mathrm{n}}_{\mathrm{RP}}\}$. The same patch pairs are determined by the threshold value of each patch $\mathrm{SP} = \{\mathrm{SP}^1, \mathrm{SP}^2, \mathrm{SP}^3, \ldots, \mathrm{SP}^n\}$. The matched keypoints in the patches are found by using the same patch pairs $\mathrm{MKP} = \{\mathrm{MKP}^1, \mathrm{MKP}^2, \mathrm{MKP}^3, \ldots, \mathrm{MKP}^n\}$.

The Matched KeyPoints MKP are combined with the segmented patches for detecting the forged regions. The unforged areas are removed efficiently by combing

MKP with the segmented patches. Initially, calculate the time TE of pixel appearance in every scale using the equation

(15) $$\mathrm{TE} = \{\mathrm{te}_{\min}, \mathrm{te}_{\min+1}, \ldots, \mathrm{te}_{\max}\},$$

where max and min represents the maximum and minimum pixel appearance rate. Due to several input image, TE value will be a random sequence and it should satisfy the condition of $\mathrm{te}_{\max} \leq n$. The unforged regions are eliminated using the standard deviation SD and mean M values which are estimated using the next equations:

(16) $$\mathrm{SD} = \sqrt{\frac{1}{\max-\min}\sum_{i=\min}^{\max}(\mathrm{te}_i - M)^2},$$

(17) $$M = \frac{1}{\max-\min}\sum_{i=\min}^{\max}\mathrm{te}_i.$$

The unforged regions are eliminated by subtracting the mean value with twice standard deviation value ($M - 2\mathrm{SD}$). The matched keypoints are merged with the segmented patches, as represented in the equation

(18) $$\mathrm{MR}(x,y) = \begin{Bmatrix} 1 & M - 2\mathrm{SD} \leq \sum_{i=1}^{n} f_i(x,y) \leq \mathrm{te}_{\max} \\ 0 & 0 \leq \sum_{i=1}^{n} f_i(x,y) < M - 2\mathrm{SD} \end{Bmatrix},$$

where $\mathrm{MR}(x,y)$ indicates merged region, $f_i(x,y)$ represents forged region and n denotes number of scales. Finally, the keypoints are combined and the forged/suspicious regions in tampered image are determined.

4. Experimental results

In copy-move forgery detection, the enhanced GWO based AlexNet model is simulated using MATLAB 2020 software environment on a computer with Intel core i7 processor, 16-GB random access memory and windows 10 (64 bit) operating system. The experimental results are validated with 5-fold cross validation technique (80:20% training and testing of data). In this application, the effectiveness of the proposed enhanced GWO based AlexNet model is analysed by comparing its performance with few existing models: adaptive segmentation and hybrid feature extraction algorithm [15], Tetrolet transform [18], Probabilistic system based on Markov random field [33], SURF feature descriptor with spatial clustering algorithm [34] and FrQZMs with modified patch matching algorithm [35] on MICC-F600, MICC-F2000, and GRIP datasets. In quantitative analysis, the proposed enhanced GWO based AlexNet model performance is evaluated using the performance measures like recall, accuracy, precision, F-score, PT, error rate, FOR, and FDR. The accuracy rate denotes the correctly recognized forged regions among all the images in the datasets. The precision rate denotes that the recognized forged region is true or not, and the recall rate states that the forged regions are correctly recognized or not. The F-score gives a single value by integrating the recall and precision rates. The mathematical expressions of detection accuracy, precision, recall, and F-score are represented in the next four equations:

(19) $$\text{Accuracy} = \frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}} \times 100\ \%,$$

(20) $$\text{Precision} = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}} \times 100\ \%,$$

(21) $$\text{Recall} = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \times 100\ \%,$$

(22) $$\text{F-score} = \frac{2\text{TP}}{2\text{TP}+\text{FN}+\text{FP}} \times 100\ \%.$$

The FOR and FDR performance measures indicate the percentage of the forged regions, which incorrectly recognized. The PT is a hypothetical screening test in copy-move forgery detection that is calculated by False Positive Rate (FPR), and True Positive Rate (TPR). The error rate represents the incorrectly recognized forged regions among all the images in the databases. The mathematical expressions of FOR, FDR, PT and error rate are indicated in the next equations:

(23) $$\text{FOR} = \frac{\text{FN}}{\text{TN}+\text{FN}} \times 100\ \%,$$

(24) $$\text{FDR} = \frac{\text{FP}}{\text{TP}+\text{FP}} \times 100\ \%,$$

(25) $$\text{PT} = \frac{\sqrt{\text{FPR}}}{\sqrt{\text{TPR}}+\sqrt{\text{FPR}}} \times 100\ \%,$$

(26) $$\text{Error rate} = 100 - \text{Accuracy},$$

where True Negative (TN) represents that the original images are correctly recognized as original images, True Positive (TP) specifies that the tampered images are correctly recognized as tampered images, False Negative (FN) states that the tampered images are incorrectly recognized as original images and False Positive (FP) rate denotes that the original images are incorrectly recognized as tampered images.

4.1. Quantitative performance with different parameter optimization techniques

In this sub-section, the performance of different hyper-parameter optimization techniques is analysed with AlexNet model on three benchmark datasets such as MICC-F600, MICC-F2000, and GRIP in light of F-score, recall, precision, and detection accuracy. By investigating Table 2, the enhanced GWO technique with AlexNet model obtained significant performance in copy-move forgery detection on MICC-F600, MICC-F2000, and GRIP datasets related to other optimization techniques such as firefly, Ant Colony Optimization (ACO) and conventional GWO technique. In the MICC-F600 dataset, the enhanced GWO based AlexNet model has achieved 99.66% of detection accuracy, 98.58% of precision, 98.48% of recall, and 99.64% of F-score, which are better compared to other hyper-parameter optimization techniques. Similarly in MICC-F2000 and GRIP databases, the proposed enhanced GWO based AlexNet model attained a maximum accuracy value of 99.75% and 98.48%, precision of 97.61% and 98.93%, recall of 97.21% and 97.13%, and F-score of 98.50% and 99.40%. The graphical presentation of different hyper-parameter optimization techniques in light of F-score, recall, precision, and detection accuracy is depicted in Fig. 2.

In Table 3, the performance of different hyper-parameter optimization techniques is analysed with AlexNet model using FDR, FOR, PT and error rate. Related to other combinations, the enhanced GWO with AlexNet model obtained a low error value on MICC-F600, MICC-F2000, and GRIP datasets. In MICC-F600 dataset, the enhanced GWO based AlexNet model achieved lower FDR value of 2.31%, FOR value of 1.16%, PT of 13.36% and error rate of 0.34%. Correspondingly in the other two datasets, the enhanced GWO based AlexNet model achieved superior performance in copy-move forgery recognition compared to other combinations:

AlexNet model with other hyper-parameter optimization techniques. Hence, the graphical presentation of different hyper-parameter optimization techniques in light of FDR, FOR, PT, and the error rate is represented in Fig. 3. In this paper, the enhanced GWO technique is proposed to optimize the hyper-parameters in AlexNet for feature extraction. The selection of suitable hyper-parameters in AlexNet improves the extraction of deep learning feature vectors for better forgery detection. For instance: the selection of an appropriate learning rate improves the model's converge rate.

Table 2. Performance evaluation with different hyper-parameter optimization techniques in light of F-score, recall, precision, and detection accuracy

AlexNet model					
Datasets	Optimizers	Accuracy (%)	Precision (%)	Recall (%)	F-score (%)
MICC-F600	Without optimization	86.55	86.94	89.51	86.26
	Firefly	71.63	58	43.68	69.13
	ACO	96.12	93.52	92.41	86.12
	GWO	95.88	93.65	95.73	96.37
	Enhanced GWO	99.66	98.58	98.48	99.64
MICC-F2000	Without optimization	81.05	92.63	96.99	84.93
	Firefly	71.40	57.25	42.98	68.27
	ACO	95.08	92.98	91.11	84.34
	GWO	95.03	93.18	94.18	94.94
	Enhanced GWO	99.75	97.61	97.21	98.50
GRIP	Without optimization	86.41	93.28	96.12	84.26
	Firefly	69.70	56.21	42.23	67.66
	ACO	94.18	93.30	91.85	85
	GWO	94.54	93.49	95.33	94.53
	Enhanced GWO	98.48	98.93	97.13	99.40

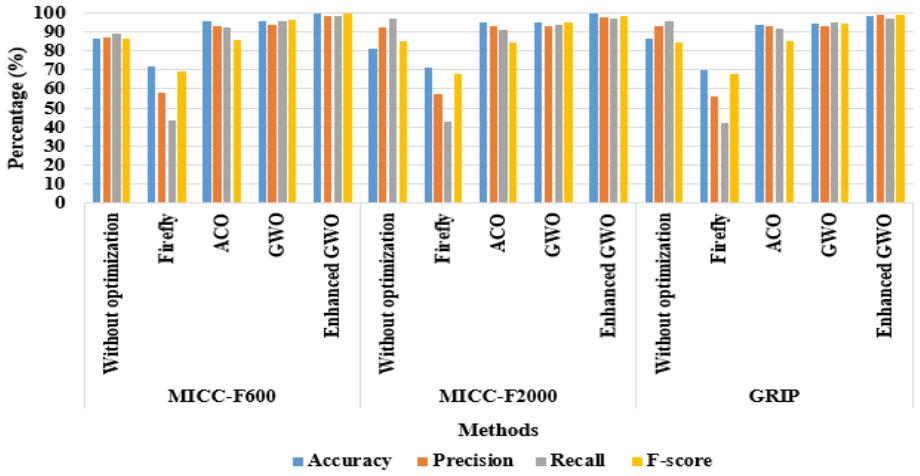


Fig. 2. Graphical presentation of different hyper-parameter optimization techniques in light of F-score, recall, precision, and detection accuracy

Table 3. Performance evaluation with different hyper-parameter optimization techniques in light of FDR, FOR, PT and error rate

AlexNet model					
Datasets	Optimizers	FDR (%)	FOR (%)	PT (%)	Error rate (%)
MICC-F600	Without optimization	6.08	6.51	16.06	13.45
	Firefly	9.26	7.47	25.48	28.37
	ACO	4.53	5.36	14.65	3.88
	GWO	3.70	1.91	14.24	4.12
	Enhanced GWO	2.31	1.16	13.36	0.34
MICC-F2000	Without optimization	7.60	7.37	16.49	18.95
	Firefly	10.74	8.89	25.04	28.60
	ACO	5.34	5.95	15.93	4.92
	GWO	4.98	3	14.16	4.97
	Enhanced GWO	3.35	2.68	12.98	0.25
GRIP	Without optimization	8.48	8.16	17.40	13.59
	Firefly	11.67	10.32	25.79	30.30
	ACO	6.48	6.63	16.79	5.82
	GWO	6.13	3.84	14.73	5.46
	Enhanced GWO	3.91	2.26	13.32	1.52

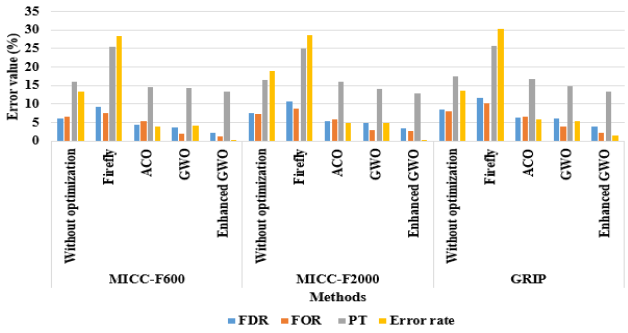


Fig. 3. Graphical presentation of different hyper-parameter optimization techniques in light of FDR, FOR, PT and error rate

4.2. Quantitative performance with different feature extraction techniques

In this sub-section the performance of different feature extraction techniques is analyzed with enhanced GWO technique on MICC-F600, MICC-F2000, and GRIP datasets by means of F-score, precision, detection accuracy, recall, FDR, FOR, PT, and error rate. By inspecting Tables 4 and 5, the combination: enhanced GWO technique with AlexNet model obtained better in copy-move forgery detection compared to other feature extraction techniques: VGG-16, VGG-19, ResNet 18, and GoogLeNet. As seen in Tables 4 and 5, the enhanced GWO based AlexNet model obtained higher detection accuracy and a lower error value on three benchmark datasets: MICC-F600, MICC-F2000, and GRIP. In this paper, the AlexNet model learns higher-level feature vectors from data in incremental manners, so there is no need for hard core feature extraction and domain expertise. The AlexNet model as a feature extractor improves the detection accuracy of learning algorithm, and reduces the computational time. The graphical representation of different feature extraction techniques in light of F-score, recall, precision, detection accuracy, FDR, FOR, PT and error rate is depicted in Figs 4 and 5.

Table 4. Performance evaluation with different feature extraction techniques in light of F-score, recall, precision and detection accuracy

Enhanced GWO technique					
Datasets	Features	Accuracy (%)	Precision (%)	Recall (%)	F-score (%)
MICC-F600	VGG-16	93.73	94.29	89.37	91.24
	VGG-19	93.03	89.71	91.16	91.73
	ResNet 18	95.03	92.56	97.48	93.72
	GoogLeNet	96.02	92.83	94.27	90.67
	AlexNet	99.66	98.58	98.48	99.64
MICC-F2000	VGG-16	93.16	93.96	89.36	91.98
	VGG-19	92.07	89.95	91.03	92.02
	ResNet 18	96.30	92.90	98.08	93.81
	GoogLeNet	97.18	93.53	94.24	90.80
	AlexNet	99.75	97.61	97.21	98.50
GRIP	VGG-16	92.47	92.64	88.72	91.15
	VGG-19	92.66	90.45	90.99	92.34
	ResNet 18	96.32	92.63	97.06	93.97
	GoogLeNet	97.15	93.32	94.19	90.74
	AlexNet	98.48	98.93	97.13	99.40

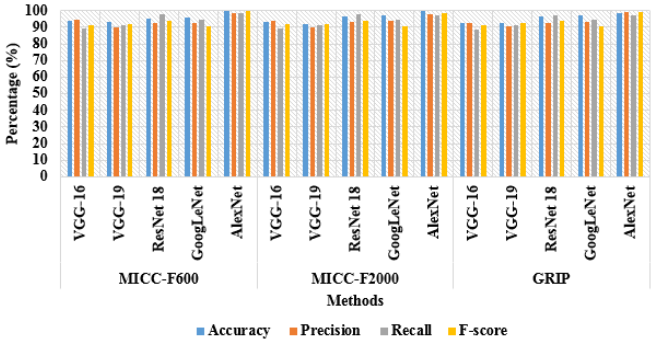


Fig. 4. Graphical presentation of different feature extraction techniques in light of F-score, recall, precision, and detection accuracy

Table 5. Performance evaluation with different feature extraction techniques in light of FDR, FOR, PT and error rate

Enhanced GWO technique					
Datasets	Features	FDR (%)	FOR (%)	PT (%)	Error rate (%)
MICC-F600	VGG-16	12.55	11.54	17.71	6.27
	VGG-19	12.79	11.06	27.50	6.97
	ResNet 18	11.24	10.55	18.08	4.97
	GoogLeNet	7.47	5.80	15.48	3.98
	AlexNet	2.31	1.16	13.36	0.34
MICC-F2000	VGG-16	12.93	12.72	18.22	6.84
	VGG-19	13.65	11.51	28.08	7.93
	ResNet 18	12.21	11.32	19.31	3.7
	GoogLeNet	7.71	6.97	16.01	2.82
	AlexNet	3.35	2.68	12.98	0.25
GRIP	VGG-16	14.19	12.71	19.35	7.53
	VGG-19	14.76	11.27	28.02	7.34
	ResNet 18	12.70	12.36	19.27	3.68
	GoogLeNet	8.16	7.56	15.53	2.85
	AlexNet	3.91	2.26	13.32	1.52

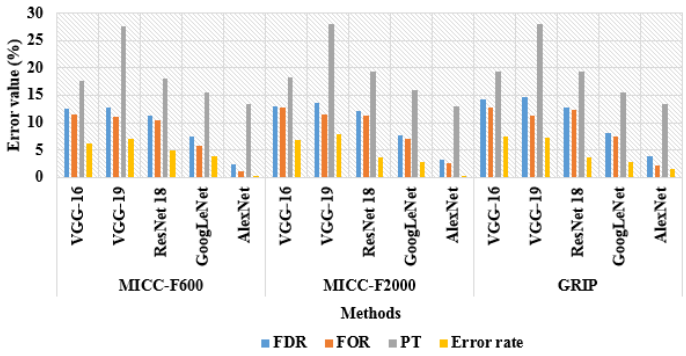


Fig. 5. Graphical presentation of different feature extraction techniques in light of FDR, FOR, PT and error rate

4.3. Quantitative performance of proposed model under different attacks

Here, the proposed enhanced GWO based AlexNet model performance is validated under different attacks like salt & pepper, Gaussian noise, rotation, blurring, and enhancement on MICC-F600, MICC-F2000 and GRIP databases by means of F-score, precision, detection accuracy, recall, FDR, FOR, PT, and error rate. In Tables 6 and 7 and Figs 6 and 7, the result is validated for rotation (30 degrees), Gaussian blur (10), enhancement (histogram equalization), salt & pepper (noise level of 0.1), and Gaussian noise (variance of 0.1 and mean of 0.2). The following attacks are detected successfully by the enhanced GWO based AlexNet model, where its results are graphically indicated in Fig. 8.

Table 6. Performance evaluation of proposed model under different attacks in light of F-score, precision, detection accuracy, and recall

Enhanced GWO based AlexNet model					
Datasets	Attacks	Accuracy (%)	Precision (%)	Recall (%)	F-score (%)
MICC-F600	Salt & pepper	77.37	74.76	80.35	82.34
	Gaussian noise	61.06	53.42	34.36	56.24
	Rotation	81.66	83.05	83.13	80.98
	Blurring	89.06	84.81	89.19	91.83
	Enhancement	84.72	93.57	95.23	86.58
MICC-F2000	Salt & pepper	75.45	81.25	90.42	72.63
	Gaussian noise	59.21	54.05	29.97	56.86
	Rotation	85.38	82	79.27	70.92
	Blurring	89.14	80.89	79.19	83.66
	Enhancement	92.78	97.48	87.21	93.01
GRIP	Salt & pepper	71.99	87.82	85.39	77.55
	Gaussian noise	69.01	47.20	40.24	57.72
	Rotation	94.11	84.85	82.22	72.57
	Blurring	86.92	80.31	87.33	91.36
	Enhancement	90.91	86.77	88.03	86.25

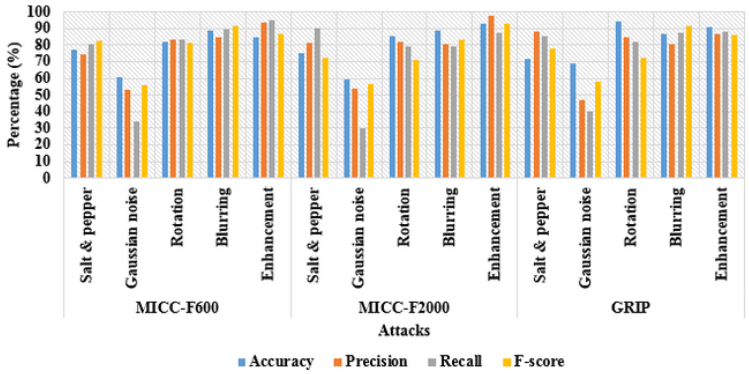


Fig. 6. Graphical analysis of proposed model under different attacks in light of F-score, precision, detection accuracy, and recall

Table 7. Performance evaluation of proposed model under different attacks in light of FDR, FOR, PT and error rate

Enhanced GWO based AlexNet model					
Datasets	Attacks	FDR (%)	FOR (%)	PT (%)	Error rate (%)
MICC-F600	Salt & pepper	18.17	16.63	21.50	22.63
	Gaussian noise	13.98	16.60	26.81	38.94
	Rotation	12.45	14.56	19.30	18.34
	Blurring	14.82	18.39	19.82	10.94
	Enhancement	17.20	12.06	17.83	15.28
MICC-F2000	Salt & pepper	10.46	14.97	25.87	24.55
	Gaussian noise	13.76	19.82	32.36	40.79
	Rotation	15.86	6.84	20.91	14.62
	Blurring	15.16	14.92	25.52	10.86
	Enhancement	13.44	4.34	20.85	7.22
GRIP	Salt & pepper	13.54	20.23	22.58	28.01
	Gaussian noise	14.35	20.27	32.75	30.99
	Rotation	12.31	17.79	24.23	5.89
	Blurring	18	18.38	19.68	13.08
	Enhancement	17.20	13.75	26.68	9.09

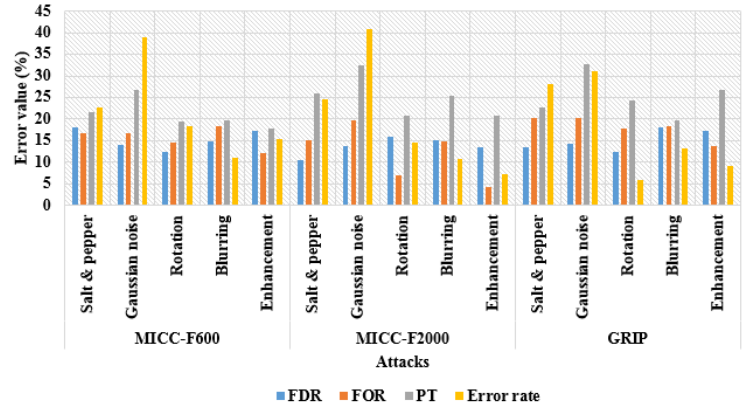


Fig. 7. Graphical analysis of proposed model under different attacks in light of FDR, FOR, PT and error rate

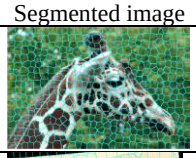
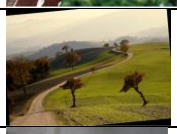
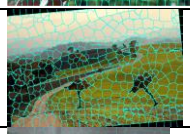
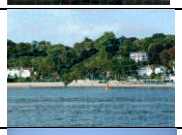
S. No	Tampered image with attacks	Segmented image	Detected forged image
a)			
b)			
c)			
d)			
e)			

Fig. 8. Results of image forged based on different attacks: Salt & pepper (a); rotation (b); Gaussian noise (c); Enhancement (d); Blurring (e)

4.4. Comparative performance and discussion

By inspecting Table 8, the proposed enhanced GWO based AlexNet model obtained better performance in forgery recognition compared to the existing models such as adaptive segmentation and hybrid Feature Extraction Algorithm [15], Tetrolet transforms [18], Probabilistic system based on Markov random field [33], SURF feature descriptor with spatial clustering algorithm [34] and FrQZMs with modified patch matching algorithm [35] on MICC-F600, MICC-F2000, and GRIP datasets in light of F-score, recall and precision. The enhanced GWO based AlexNet model almost showed 1.5% to 6% improvement in forgery detection compared to the existing models by means of precision. Correspondingly, the proposed enhanced GWO based AlexNet model obtained higher recall and F-score values related to the comparative models.

Table 8. Comparative investigation between the proposed and existing models

Models	Dataset	Precision (%)	Recall (%)	F-score (%)
Adaptive segmentation and hybrid feature extraction algorithm [15]	MICC-F600	92.45	93.67	92.75
Tetrolet transform [18]	GRIP	97.56	-	98.76
Probabilistic system based on Markov random field [33]	MICC-F600	-	84.37	-
SURF with spatial clustering algorithm [34]	MICC-F2000	96.83	95.24	96.03
FrQZMs with modified patch matching algorithm [35]	GRIP	-	-	95.33
Enhanced GWO based AlexNet model	MICC-F600	98.58	98.48	99.64
	MICC-F2000	97.61	97.21	98.50
	GRIP	98.93	97.13	99.40

The obtained experimental results showed that the proposed model effectively detects the copy-move forgeries involved in a smooth and small region. Additionally, the enhanced GWO based AlexNet model significantly classifies the naturally identical regions and copy-move regions. As stated earlier, the inclusion of the enhanced GWO technique in the AlexNet model diminishes the running time and improves the converge rate of the model. By seeing Table 9, the enhanced GWO technique with AlexNet model achieved limited running time compared to other optimization techniques on MICC-F600, MICC-F2000 and GRIP datasets.

Table 9. Performance evaluation in terms of running time

Optimizers	Dataset	Patch Segmentation (s)	Feature extraction (s)	Matching (s)	Total (s)
Firefly	MICC-F600	9.41	19.07	10.87	39.35
	MICC-F2000	7.86	15.63	10.35	33.84
	GRIP	7.05	12.97	8.78	28.81
ACO	MICC-F600	2.83	12.39	4.29	19.51
	MICC-F2000	1.58	9.27	4.13	14.98
	GRIP	0.63	6.46	3.11	10.20
Enhanced GWO	MICC-F600	0.88	6.15	2.11	9.14
	MICC-F2000	0.32	4.62	1.87	6.81
	GRIP	0.11	3.21	1.03	4.35

5. Conclusion

In this paper, a new enhanced GWO based AlexNet model is introduced for effective copy-move forgery detection. Firstly, a superpixel clustering algorithm is used for patch segmentation in the tampered images. Further, an enhanced GWO based AlexNet model is proposed to extract features from the different scales of segmented patches that are used for re-constructing the dense depth of the image pixels. This action eases the process of matching the forged region with the original region. Finally, an adaptive patch matching algorithm is used to locate the suspicious regions in the tampered images. As seen in the resulting phase, the enhanced GWO based AlexNet model achieved higher accuracy of 99.66%, 99.75% and 98.48% on MICC-F600, MICC-F2000, and GRIP databases. In addition, the enhanced GWO based AlexNet model showed good performance in forgery detection related to comparative models in light of precision, recall, and F-score. The experimental outcomes showed that the proposed enhanced GWO based AlexNet model accurately detects and locates the forged regions, even under the conditions of salt & pepper noise, Gaussian noise, rotation, blurring, and enhancement. The proposed model detects multiple forgery cases and small tampered regions, even while the tampered image is smooth. As a future extension, the hybrid deep learning based feature descriptor is included in the proposed model for further enhancement of forgery detection.

References

1. Wang, X. Y., C. Wang, L. Wang, L. X. Jiao, H. Y. Yang, P. P. Niu. A Fast and High Accurate Image Copy-Move Forgery Detection Approach. – Multidimensional Systems and Signal Processing, Vol. **31**, 2020, pp. 857-883.
https://doi.org/10.1007/s11045-019-00688-x

2. M a h m o o d, T., Z. M e h m o o d, M. S h a h, T. S a b a. A Robust Technique for Copy-Move Forgery Detection and Localization in Digital Images via Stationary Wavelet and Discrete Cosine Transform. – Journal of Visual Communication and Image Representation, Vol. **53**, 2018, pp. 202-214.
https://doi.org/10.1016/j.jvcir.2018.03.015
3. W u, Y., W. A b d-A l m a g e e d, P. N a t a r a j a n. Image Copy-Move Forgery Detection via an End-to-End Deep Neural Network. – In: Proc. of IEEE Winter Conference on Applications of Computer Vision (WACV'18), IEEE, 12-15 March 2018, Lake Tahoe, NV, USA, pp. 1907-1915. DOI: 10.1109/WACV.2018.00211.
4. M a h m o o d, T., A. I r t a z a, Z. M e h m o o d, M. T. M a h m o o d. Copy-Move Forgery Detection through Stationary Wavelets and Local Binary Pattern Variance for Forensic Analysis in Digital Images. – Forensic Science International, Vol. **279**, 2017, pp. 8-21. DOI: 10.1016/j.forsciint.2017.07.037.
5. J i n, G., X. W a n. An Improved Method for SIFT-Based Copy-Move Forgery Detection Using Non-Maximum Value Suppression and Optimized J-Linkage. – Signal Processing: Image Communication, Vol. **57**, 2017, pp. 113-125.
https://doi.org/10.1016/j.image.2017.05.010
6. B i, X., C. M. P u n. Fast Reflective Offset-Guided Searching Method for Copy-Move Forgery Detection. – Information Sciences, Vol. **418-419**, 2017, pp. 531-545.
https://doi.org/10.1016/j.ins.2017.08.044
7. Z h o n g, J. L., C. M. P u n, Y. F. G a n. Dense Moment Feature Index and Best Match Algorithms for Video Copy-Move Forgery Detection. – Information Sciences, Vol. **537**, 2020, pp. 184-202.
https://doi.org/10.1016/j.ins.2020.05.134
8. I s l a m, A., C. L o n g, A. B a s h a r a t, A. H o o g s. DOA-GAN: Dual-Order Attentive Generative Adversarial Network for Image Copy-Move Forgery Detection and Localization. – In: Proc. of IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 2020, pp. 4675-4684. DOI: 10.1109/CVPR42600.2020.00473.
9. Y a n g, B., X. S u n, H. G u o, Z. X i a, X. C h e n. A Copy-Move Forgery Detection Method Based on CMFD-SIFT. – Multimedia Tools and Applications, Vol. **77**, 2019, pp. 837-855.
https://doi.org/10.1007/s11042-016-4289-y
10. H o s n y, K. M., H. M. H a m z a, N. A. L a s h i n. Copy-Move Forgery Detection of Duplicated Objects Using Accurate PCET Moments and Morphological Operators. – The Imaging Science Journal, Vol. **66**, 2018, pp. 330-345.
https://doi.org/10.1080/13682199.2018.1461345
11. D i x i t, R., R. N a s k a r, S. M i s h r a. Blur-Invariant Copy-Move Forgery Detection Technique with Improved Detection Accuracy Utilizing SWT-SVD. – IET Image Processing, Vol. **11**, 2011, pp. 301-309. DOI: 10.1049/iet-ipr.2016.0537.
12. W a n g, C., Z. Z h a n g, X. Z h o u. An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features. – Symmetry, Vol. **10**, 2018, pp. 706.
https://doi.org/10.3390/sym10120706
13. A l-Q e r s h i, O. M., B. E. K h o o. Enhanced Block-Based Copy-Move Forgery Detection Using k-Means Clustering. – Multidimensional Systems and Signal Processing, Vol. **30**, 2019, pp. 1671-1695.
https://doi.org/10.1007/s11045-018-0624-y
14. A b d a l l a, Y., M. T. I q b a l, M. S h e h a t a. Copy-Move Forgery Detection and Localization Using a Generative Adversarial Network and Convolutional Neural-Network. – Information, Vol. **10**, 2019, pp. 286.
https://doi.org/10.3390/info10090286
15. T i n n a t h i, S., G. S u d h a v a n i. An Efficient Copy Move Forgery Detection Using Adaptive Watershed Segmentation with AGSO and Hybrid Feature Extraction. – Journal of Visual Communication and Image Representation, Vol. **74**, 2020, 102966.
https://doi.org/10.1016/j.jvcir.2020.102966
16. K a s b a n, H., S. N a s s a r. An Efficient Approach for Forgery Detection in Digital Images Using Hilbert-Huang Transform. – Applied Soft Computing, Vol. **97**, pp. 106728.
https://doi.org/10.1016/j.asoc.2020.106728

17. E l a s k i l y, M. A., H. A. E l n e m r, A. S e d i k, M. M. D e s s o u k y, G. M. E l B a n b y, O. A. E l s h a k a n k i r y, A. A. M. K h a l a f, H. K. A s l a n, O. S. F a r a g a l l a h, F. E. A. E l-S a m i e. A Novel Deep Learning Framework for Copy-Move Forgery Detection in Images. – Multimedia Tools and Applications, Vol. **79**, 2020, pp. 19167-19192. **https://doi.org/10.1007/s11042-020-08751-7**
18. M e e n a, K. B., V. T y a g i. A Copy-Move Image Forgery Detection Technique Based on Tetrolet Transform. – Journal of Information Security and Applications, Vol. **52**, 2020, pp. 102481. **https://doi.org/10.1016/j.jisa.2020.102481**
19. A g a r w a l, R., O. P. V e r m a. An Efficient Copy Move Forgery Detection Using Deep Learning Feature Extraction and Matching Algorithm. – Multimedia Tools and Applications, Vol. **79**, 2019, pp. 7355-7376. **https://doi.org/10.1007/s11042-019-08495-z**
20. Z h u, Y., C. C h e n, G. Y a n, Y. G u o, Y. D o n g. AR-Net: Adaptive Attention and Residual Refinement Network for Copy-Move Forgery Detection. – IEEE Transactions on Industrial Informatics, Vol. **16**, 2020, pp. 6714-6723. DOI: 10.1109/TII.2020.2982705.
21. L i u, Y., Q. G u a n, X. Z h a o. Copy-Move Forgery Detection Based on Convolutional Kernel Network. – Multimedia Tools and Applications, Vol. **77**, 2018, pp. 18269-18293. **https://doi.org/10.1007/s11042-017-5374-6**
22. L i n, C., W. L u, X. H u a n g, K. L i u, W. S u n, H. L i n, Z. T a n. Copy-Move Forgery Detection Using Combined Features and Transitive Matching. – Multimedia Tools and Applications, Vol. **78**, 2018, pp. 30081-30096. **https://doi.org/10.1007/s11042-018-6922-4**
23. A l b e r r y, H. A., A. A. H e g a z y, G. I. S a l a m a. A Fast SIFT Based Method for Copy Move Forgery Detection. – Future Computing and Informatics Journal, Vol. **3**, 2018, pp. 159-165. **https://doi.org/10.1016/j.fcij.2018.03.001**
24. Y a n g, F., J. L i, W. L u, J. W e n g. Copy-Move Forgery Detection Based on Hybrid Features. – Engineering Applications of Artificial Intelligence, Vol. **59**, 2017, pp. 73-83. **https://doi.org/10.1016/j.engappai.2016.12.022**
25. N i y i s h a k a, P., C. B h a g v a t i. Copy-Move Forgery Detection Using Image Blobs and BRISK Feature. – Multimedia Tools and Applications, Vol. **79**, 2020, pp. 26045-26059. **https://doi.org/10.1007/s11042-020-09225-6**
26. H u a n g, H. Y., A. J. C i o u. Copy-Move Forgery Detection for Image Forensics Using the Superpixel Segmentation and the Helmert Transformation. – EURASIP Journal on Image and Video Processing, 2019, pp. 689. **https://doi.org/10.1186/s13640-019-0469-9**
27. W a n g, C., Z. Z h a n g, Q. L i, X. Z h o u. An Image Copy-Move Forgery Detection Method Based on SURF and PCET. – IEEE Access, Vol. **7**, 2019, pp. 170032-170047. DOI: 10.1109/ACCESS.2019.2955308.
28. R a j u, P. M., M. S. N a i r. Copy-Move Forgery Detection Using Binary Discriminant Features. – Journal of King Saud University-Computer and Information Sciences, 2018. **https://doi.org/10.1016/j.jksuci.2018.11.004**
29. G a n i, G., F. Q a d i r. A Robust Copy-Move Forgery Detection Technique Based on Discrete Cosine Transform and Cellular Automata. – Journal of Information Security and Applications, Vol. **54**, 2020, pp. 102510. DOI: 10.1016/j.jisa.2020.102510.
30. S o n i, B. P. K., D a s, D. M. T h o u n a o j a m. Geometric Transformation Invariant Block Based Copy-Move Forgery Detection Using Fast and Efficient Hybrid Local Features. – Journal of Information Security and Applications, Vol. **45**, 2019, pp. 44-51. DOI: 10.1016/j.jisa.2019.01.007.
31. C h e n, C. C., W. Y. L u, C. H. C h o u. Rotational Copy-Move Forgery Detection Using SIFT and Region Growing Strategies. – Multimedia Tools and Applications, Vol. **78**, 2019, pp. 18293-18308. **https://doi.org/10.1007/s11042-019-7165-8**
32. P a r k, J. Y., T. A. K a n g, Y. H. M o o n, I. K. E o m. Copy-Move Forgery Detection Using Scale Invariant Feature and Reduced Local Binary Pattern Histogram. – Symmetry, Vol. **12**, 2020, pp. 492. **https://doi.org/10.3390/sym12040492**

33. E l h a m i n i a, B., A. H a r a t i, A. T a h e r i n i a. A Probabilistic Framework for Copy-Move Forgery Detection Based on Markov Random Field. – Multimedia Tools and Applications, Vol. **78**, (2019), pp. 25591-25609.
https://doi.org/10.1007/s11042-019-7713-2
34. B i l a l, M., H. A. H a b i b, Z. M e h m o o d, R. M. Y o u s a f, T. S a b a, A. R e h m a n. A Robust Technique for Copy-Move Forgery Detection from Small and Extremely Smooth Tampered Regions Based on the DHE-SURF Features and mDBSCAN Clustering. – Australian Journal of Forensic Sciences, Vol. **53**, 2021, pp. 459-482.
https://doi.org/10.1080/00450618.2020.1715479
35. C h e n, B., M. Y u, Q. S u, H. J. S h i m, Y. Q. S h i. Fractional Quaternion Zernike Moments for Robust Color Image Copy-Move Forgery Detection. – IEEE Access, Vol. **6**, 2018, pp. 56637-56646. DOI: 10.1109/ACCESS.2018.2871952.
36. C o z z o l i n o, D., G. P o g g i, L. V e r d o l i v a. Efficient Dense-Field Copy-Move Forgery Detection. – IEEE Transactions on Information Forensics and Security, Vol. **10**, 2015, pp. 2284-2297. DOI: 10.1109/TIFS.2015.2455334.
37. A m e r i n i, I., L. B a l l a n, R. C a l d e l l i, A. D. B i m b o, G. S e r r a. A Sift-Based Forensic Method for Copy-Move Attack Detection and Transformation Recovery. – IEEE Transactions on Information Forensics and Security, Vol. **6**, 2011, pp. 1099-1110. DOI: 10.1109/TIFS.2011.2129512.
38. M a, J., X. W a n g, B. X i a o. An Image Segmentation Method Based on Simple Linear Iterative Clustering and Graph-Based Semi-Supervised Learning. – In: Proc. of International Conference on Orange Technologies (ICOT'15), IEEE, Hong Kong, China, 2015, pp. 10-13. DOI: 10.1109/ICOT.2015.7498477.
39. H e g d e, R. B., K. P r a s a d, H. H e b b a r, B. M. K. S i n g h. Feature Extraction Using Traditional Image Processing and Convolutional Neural Network Methods to Classify White Blood Cells: A Study. – Australasian Physical & Engineering Sciences in Medicine, Vol. **42**, 2017, pp. 627-638.
https://doi.org/10.1007/s13246-019-00742-9
40. G o e l, T., R. M u r u g a n, S. M i r j a l i l i, D. K. C h a k r a b a r t t y. OptCoNet: An Optimized Convolutional Neural Network for an Automatic Diagnosis of COVID-19. – Applied Intelligence, Vol. **51**, 2021, pp. 1351-1366.
https://doi.org/10.1007/s10489-020-01904-z
41. W u, C., J. W a n g, X. C h e n, P. D u, W. Y a n g. A Novel Hybrid System Based on Multi-Objective Optimization for Wind Speed Forecasting. – Renewable Energy, Vol. **146**, 2020, pp. 149-165. DOI: 10.1016/j.renene.2019.04.157.

Received: 31.01.2022; Second Version: 08.08.2022; Accepted: 25.08.2022