Multimedia Research



Received 17 December, Revised 22 February, Accepted 18 March

# Face Image Forgery Detection by Weight Optimized Neural Network Model

R. Cristin Department of CSE St.Joseph College of Engineering Choondacherry, Kerala, India rcristin2015@gmail.com **Dr.V. Cyril Raj** Department of CSE Dr.M.G.R University Chennai, Tamil Nadu, India Ramalatha Marimuthu Department of CSE Sri Krishna college of engineering and technology Coimbatore, Tamil Nadu, India

Abstract: This framework introduces a new automatic image forgery detection approach that involves four main stages like (i) Illumination map computation, (ii) Face detection, (iii) Feature extraction, and (iv) Classification. Initially, the processing of input image is exploited by means of illumination map estimation, which acquires two computation processes called Gray world estimates and Inverse-Intensity chromaticity. Subsequent to this, the Viola-Jones algorithm is employed for the face detection process, which is the second phase, in order to detect the face image clearly. Once after the detection process, the obtained facial image is subjected to feature extraction. For this, Grey Level Co-occurrence Matrix (GLCM) is exploited that extract the facial features from the image. After this, the classification process is carried out for the extracted facial features by employing the Neural Network (NN) classifier. On the whole, this paper mainly concerned over the optimization concept, in which the weight of the NN is optimally selected by using the renowned optimization algorithm named Whale Optimization Algorithm (WOA). To the end, the performance of the implemented model is compared over the other classical models like k-nearest neighbor (kNN), NN and Support Vector Machine (SVM) regarding certain measures like Accuracy, Sensitivity, and Specificity.

Keywords: Face Recognition; Viola-Jones Algorithm; Feature Extraction; Classification; Optimization

# 1. Introduction

In recent times, the communication media has fed up with images. According to the belief, all know that the image depicts more truth on any situation or incident than words. On taking the past, the images have to be manipulated based on the professional knowledge that produced by classical film cameras having complicated dark-room equipment that makes critical to average users. The attainment of the image is easier then because of the economical devices. Thereby made possible to record, store and share the large count of images. Nowadays the digital image plays a significant role in human life. Because of the enormous growth in the image processing methods, with the availability of image modification tools any modification in the images can be done. These modifications cannot be recognized by human eyes. Hence, identification of the image integrity is very important in today"s life.

Many image processing [13] [15] techniques have been introduced in this advance era of digital images. As the same, the digital image forgery detection is also on increase as because of the increase in image editing software tools.

The software tools are used to edit the images and they undergo various processing steps and hence seemed so photorealistic that the normal human eyes cannot detect the forgery that made over the image. Because of this corollary, the appearance of manipulated images is on increase rate whereby directs to reduce in trust over the visual content. Therefore, image authenticity is not given as granted. The originality of the image information is provoked now with the technological advancement of forgery tools.

Hence, an alternative path is determined by the research community to authenticate the image and called it digital image forensics. One of the authentication techniques is the forgery detection technique that considers the original image has posed inherent patterns, where several imaging devices or the processing is presented. As because of the sophisticated and advanced processing tools, the image forgery detection [11] [12] [14] has become complicated. On this case, various current approaches are evolved by the researchers for detecting the forgery within the image.

This work has attempted to introduce a new automatic image forgery detection approach using four phases namely, (i) Illumination map computation, (ii) Face detection, (iii) Feature extraction, and (iv)Classification. Illumination map estimation is the first phase, which has two processes. The Viola-Jones algorithm is adopted for the face detection process and the feature extraction is made by using the GLCM structure. The next step is classification, where the classification of extracted features is done using NN classifier. Finally, the optimization process is involved, which optimizes the weight of NN by deploying the WOA algorithm. This paper is organized as follows: Section 2 defines the Literature review on image forgery detection. Section 3 explains the proposed forgery detection model. Section 4 depicts Whale Optimization based NN training. Section 5 delineates the results and their discussions. Section VI ends the paper.

### 2 Literature Survey

#### 2.1 Related Works

In 2017, Farooq *et al.* [1] have proposed an approach to detect the image forgery with multiple types. Here, an image forgery technique has been developed based on spatial rich model (SRM) with local binary pattern (LBP). For examining the performance-to-model dimensionality trade-off, diverse submodel selection structures were introduced and reviewed. The feature was classified as diverse forgery classes by means of Ensemble multi-class classifier. The simulation of the proposed structure has been evolved from IEEE IFS-TC image forensics dataset that was comprised of 10 various forgeries type. The outcome has revealed that the implemented model has better efficiency with the accuracy of 98.4%.

In 2017, Jeronymo *et al.* [2] have presented a model for image forgery detection, named error level analysis (ELA) in lossy compressed digital images and the automatic wavelet soft-thresholding were used to filter the noisy components. The recompression of the lossy compressed image was made with ELA at an identified error rate and the computation of absolute differences among these images called error levels was made. This paper has implemented the lowpass filter via wavelet thresholding. Where attenuates the error level noises. This paper has the main concentration on examining the Daubechies wavelets with semi-automatic soft-thresholding for enlightening the image forgeries.

In 2016, Oommen *et al.* [3] have introduced a hybrid model on the basis of singular value decomposition (SVD) and local fractal dimension (LFD) for effective localization and detection of image's duplicated regions. Initially, the image was segmented as fixed size blocks and has computed the local fractal dimension. The inherent computational complexity of fractal approaches has been decreased by arranging the image blocks in the B+ tree on the basis of LFD values. By deploying the singular values, block pairs in every segment have been compared, in order to determine the regions that demonstrate the increased similitude. The experimental outcome has demonstrated that the implemented model has effective performance in the detection of multiple forgeries inside the image.

In 2015, Pun *et al.* [4] have proposed the narrative copy-move forgery detection technique by means of feature point matching and adaptive over-segmentation. The implemented structure has incorporated the keypoint-based and block-based forgery detection approaches. Initially, the segmentation of the host image has been made as irregular blocks and nonoverlapping adaptively using the adaptive over-segmentation method. After that, the extraction of feature points from every block was made for indicating the suspected forgery regions approximately. For the precise detection of forgery regions, the forgery region extraction approach was introduced that substitutes the small superpixels for feature points. Now the neighboring blocks were merged for generating the merged regions. To the end, the merged regions were applied with the morphological operation, in order to produce the detected forgery regions. The analysis has explained that the implemented model has superior detection outcomes than any other forgery detection approaches.

In 2018, Mayer *et al.* [5] have developed a narrative method on the basis of perceiving localized Lateral Chromatic Aberration (LCA) inconsistencies for detecting the regions of the forged image. For this purpose, a statistical approach has been proposed for capturing the inconsistency among the local and global estimates of LCA. This method has been used as a preposition testing problem in forgery detection and extracts the detection statistic. A sequence of investigation has been made to examine the detection efficacy. Further, a new and effective LCA estimation method has been proposed. In order to attain this, a block matching approach namely diamond search was adopted. The experimental analysis has shown that the implemented model has decreased tome on estimation with no presentation of extra estimation error.

#### **3 Proposed Forgery Detection Model**

In this research work, a new automatic image forgery detection approach is proposed, which consist of four stages namely, (i) Illumination map computation, (ii) Face detection, (iii) Feature extraction, and (iv) Classification. Firstly, the input image is processed by illumination map which adapts two computation processes. The next step is the face detection process, where the Viola-Jones algorithm is deployed to detect the face from the image. After the face detection process, the input is subjected to feature extraction. In this, GLCM [20] and LVP based feature extraction are exploited to extract the facial image features. The final step is the classification, where the extracted facial features are classified using the NN classifier. The main objective of this framework defines the optimization concept, where the selection of optimal weight in NN is made. For this purpose, a renowned meta-heuristic optimization algorithm is deployed, named WOA. Fig. 1 illustrates the overall artwork of the proposed image forgery detection approach.



Fig 1. Art of the proposed image forgery detection model

#### **3.1 Computation of Illumination Map**

This section is about the estimation on the illumination map. The Felzenszwalb and Huttenlocher [6] are used for the segmentation of superpixels that appeared from the input image. The entire individual superpixels exploit the illumination color. The color estimators such as grey world estimates and inverse-intensity chromaticity space are deployed for evaluating the illumination.

Grey world estimates: The average scene color is considered to be grey and therefore, the average grey gets deviates in accordance with the illumination. Consider the RGB (red, green, blue) colors of a pixel placed at x and are given in Eq. (1).

$$F(x) = [F_{R}(x), F_{G}(x), F_{B}(x)]$$
(1)

It is considered to be a linear camera response and truly diffuse reflection and hence is stated in Eq. (2).

$$F(x) = \int c(\lambda, x) m(\lambda, x) S(\lambda) d\lambda$$
(2)

In this, the visible light spectrum is defined with  $\eta$ , the light's wavelength is  $\lambda$ , illuminant spectrum is denoted as  $c(\lambda, x)$ , and the surface reflectance is represented by  $F_G(x)$ .  $S(\lambda)$  is the camera sensitivity to color. Based on the manipulation of three parameters, the world grey hypothesis is extended and the parameters are smoothing parameter  $\sigma$ , the order of the derivative p and norm of Minkowski  $\rho$ . The illuminant color c is given in Eq. (3).

$$\operatorname{Rc}^{p,p,\sigma} = \left( \int \left| \frac{\partial^{p} F^{\sigma}(x)}{\partial x^{p}} \right|^{p} dx \right)^{\frac{1}{p}}$$
(3)

In this, the pixel coordinates are given by x, the scaling factor is R, and the absolute value is depicted as  $| \cdot |$ . The monitored intensity at a position x that smoothened by the kernel  $\sigma$  is  $F^{\sigma}(x)$  and the

differentiation is delineated as  $\partial$ . For the color channel, the parameter c is individually evaluated and thus the robustness is enhanced by derivative operators.

Inverse-intensity chromaticity: In contrast to grey world estimates, this technique made an assumption to demonstrate the specular reflectance and diffuse. Assume Eq. (1) and that function is depicted in Eq. (4).

$$\mathbf{F}(\mathbf{x}) = [\mathbf{F}_{\mathrm{R}}(\mathbf{x}), \mathbf{F}_{\mathrm{G}}(\mathbf{x}), \mathbf{F}_{\mathrm{B}}(\mathbf{x})]^{\mathrm{T}}$$
(4)

The connection among color channel chromaticity  $\gamma_S(x)$ , function F(x) and illuminated channel chromaticity  $\chi_S$  is given as per the Eq. (5).

$$\gamma_{\rm S}(x) = n(x) \times \frac{1}{\sum_{j \in \{\rm R,G,B\}} F_j(x)} + \chi_{\rm S}$$
(5)

The geometric influence is denoted by the function n(x) that is not analytically computed, yet goes through a suitable solution. Hence, for identifying the illuminant color is made only through y-intercept  $\chi_s$ , which finds by analyzing the pixel.

#### 3.2 Viola-Jones based Face Detection

The Viola-Jones algorithm [7] is considered as the fast and efficient algorithm on detecting the face and has the computational speed just in milliseconds. At first, the results are differentiated with the threshold value, once after subtracting the marked black pixels from the white pixels, so that the identification of features is performed on the basis of this criteria. The following are the phases involved in the Viola-Jones algorithm.

(a) Haar-based features [16]: The white and clack portion of the image is determined by this, which exploits the rectangle around the face.

(b) Integral image formation [17]: the formation of an integral image is made by the summation of individual pixel's value with its neighbor's pixel value. it can also be defined as the individual pixel's value is exploited by adding the four neighbor's pixel value which gathers within the rectangle area.

(c) Adaboost machine-learning approach [18]: the machine -learning approach based on the bagging concept is named as AdaBoost and is mainly employed for the face detection process. The AdaBoost algorithm is used for selecting the few facial features, whereby makes the computation fast and easier. This is assumed as having greater significance as it eliminates the unwanted background.

(d) Cascade classifier [19] to concatenate the features: It composed of numerous classifiers that permit the selection of the face image. The classifier is given with sub-windows so that, it can examine every sub-window to have the face or not.

Hence, the face detection from the image is successfully made using the Viola-Jones algorithm and is then given to the feature extraction process.

#### 3.3 GLCM based Feature Extraction

The face-detected image is given as the input to the feature extraction process that made based on GLCM [8]. The GLCM algorithm is given as follows: The matrix that explains the diverse grouping distribution within the pixel brightness values i.e. grey level which occurs inside an image is termed as GLCM. The image's texture characteristics on information are gained using GLCM. The spatial correlation at orientation angle and precise distance among the two pixels is performed by taking the GLCM texture into consideration. Basically, a matrix co-occurrence is formed by means of GLCM within an image data, by which the feature's matrix function might be gained. The following are the GLCM properties.

**Contrast**: It is further called as a summation of squares variance, which defines the evaluation of intensity contrast among the pixel and its neighbour within the whole image. Moreover, the summation of diversity is also measured in the image's grey level. Eq. (6) delineates the evaluation of the contrast value.

$$Contrast = \sum_{a,b=1}^{N} V_{a,b} (a-b)^2$$
(6)

**Energy or Uniformity:** It quantifies to analyze the intensity in GLCM's gray level concentration. The summation of squared elements in GLCM is given here. The evaluation of the energy value is in Eq. (7).

$$Energy = \sum_{a,b=1}^{N} V_{a,b}^{2}$$
(7)

Multimedia Research

**Homogeneity:** Inverse Difference Moment is considered as the sharing of proximity measure within the elements over GLCM diagonal from the GLCM. The contrast value's inverse is termed as Homogeneity values and is given in Eq. (8).

Homogeneity = 
$$\frac{\sum_{a,b=1}^{N} V_{a,b}}{1 + (a - b)^2}$$
(8)

**Correlation:** An index by which the reference pixel is associated to the pixel in the distance and direction of the whole image is referred as correlation of the pixel. The evaluation of this correlation value is made as per Eq. (9), where, the mean and variance are exploited by Eq. (10) and (11).

$$Correlation = \sum_{a,b=1}^{N} \frac{(a - \mu_a)(b - \mu_b)}{\sigma_a \sigma_b} V_{a,b}$$
(9)

$$\mu_{a} = \sum_{a=1}^{d} \hat{p} \sum_{b=1}^{d} V_{a,b} , \ \mu_{b} = \sum_{b=1}^{d} b \sum_{a=1}^{d} V_{a,b}$$
(10)

$$\sigma_{a} = \sum_{a=1}^{d} (a - \mu_{a})^{2} \sum_{b=1}^{d} V_{a,b}$$

$$\sigma_{b} = \sum_{b=1}^{d} (b - \mu_{b})^{2} \sum_{a=1}^{d} V_{a,b}$$
(11)

In this, the horizontal coordinates and vertical coordinates matrix is depicted as a and b, and the matrix value in a and b coordinate is given as  $V_{a,b}$ . Finally, after this feature extraction process, the extracted features from the image are obtained.

#### **3.4 Classification**

NN [9] classifier is deployed to classify the extracted facial images for detecting the forgeries. NN is explained by the following Eq. (12), (13) and (14). where i refers to the hidden neuron, the bias weight to  $i^{th}$  hidden neuron is given by  $\operatorname{wt}_{(\widetilde{bi})}^{(\mathrm{HI})}$ , the count of input neurons is depicted by  $I_{(n)}$ , the count of hidden neurons is denoted as  $HI_{(n)}$ ,  $\operatorname{wt}_{(\widetilde{bk})}^{(0)}$  expresses the output bias weight to  $k^{th}$  layer,  $\operatorname{wt}_{(ik)}^{(0)}$  symbolizes the output weight from  $i^{th}$  hidden neuron to  $k^{th}$  layer,  $\operatorname{wt}_{(\mathrm{li})}^{(\mathrm{HI})}$  terms as the weight from  $l^{th}$  input to  $i^{th}$  hidden neuron and AF refers to the activation function.  $\overline{OP}_k$  is the network output, predicted output and it is

neuron and AF refers to the activation function.  $OP_k$  is the network output, predicted output and it is given in Eq. (14),  $OP_k$  is the actual output.

$$\overline{\mathrm{HO}}^{(\mathrm{HI})} = \mathrm{AF}\left(\mathrm{wt}_{\left(\widetilde{\mathrm{bi}}\right)}^{(\mathrm{HI})} + \sum_{l=1}^{l_{(\mathrm{n})}} \mathrm{wt}_{\left(\mathrm{li}\right)}^{(\mathrm{HI})}(\mathrm{Inputfeatures})\right)$$
(12)

$$\overline{OP}_{k} = AF \left( wt_{(\widetilde{b}k)}^{(o)} + \sum_{i=1}^{HI_{(n)}} wt_{(ik)}^{(o)} \overline{HO}_{i}^{(HI)} \right)$$
(13)

$$\mathbf{ER}^{*} = \underset{\left\{\mathbf{wt}_{\left(\widetilde{bi}\right)}^{(\mathrm{HI})}, \mathbf{wt}_{\left(\widetilde{bi}\right)}^{(\mathrm{o})}, \mathbf{wt}_{\left(\widetilde{bk}\right)}^{(\mathrm{o})}, \mathbf{wt}_{\left(\widetilde{bk}\right)}^{(\mathrm{o})}\right\}}{\operatorname{arg\,min}} \sum_{k=1}^{O(n)} |OP_{k} - \overline{OP}_{k}|$$
(14)

The output of the NN is the classified output.

## 4. Whale Optimization Based NN Training

#### 4.1 Solution Encoding and Objective Function

The main objective of this research work is to attain precise classification accuracy, and it can be achieved only if the Error rate  $ER^*$  gets minimized. Hence for this purpose, this research work exhibits the optimal weight wt:  $wt \rightarrow wt_{(bi)}^{(HI)}, wt_{(bi)}^{(o)}, wt_{(bi)}^{(o)}, wt_{(bi)}^{(o)}$  of NN by deploying an optimization concept that uses the renowned whale optimization algorithm. The input solution that is given to the proposed model is given in Fig. 2.



Fig 2. Solution Encoding

#### 4.2 Whale Optimization Algorithm

WOA [10] is one of the present optimization algorithms inspired by nature that works on the basis of humpback whales. This algorithm is developed based on the bubble-net feeding approach of the whales that are recognized as the hunting behaviour. The arithmetical depiction of WOA algorithm is as follows:

Shrinking encircling mechanism: When hunting the prey's, the whale can determine the prey's current location and they encircle them. The target prey captured by them is depicted as the recent best solution. Concurrently, the optimal solution is attained by updating the position. Eq. (15) and (16) predicts the whale's encircling behaviour.

$$\vec{\mathbf{D}} = \left| \vec{\mathbf{Z}} \cdot \vec{\mathbf{H}}^*(\mathbf{t}) - \vec{\mathbf{H}} \mathbf{t} \right| \tag{15}$$

$$\vec{H}(t+1) = \vec{H}^{*}(t) - \vec{Q}.\vec{D}$$
(16)

In this, the present iteration is given as t, the coefficient vectors are expressed by Q and Z, the best solution's position vector is depicted as  $H^*$  and the vector's position is portrayed as H, the absolute value is delineated as  $| \cdot |$ , the element-by-element multiplication is enabled using "." function.

On every iteration,  $H^*$  requires to be updated on the condition, such that if subsist any better solution. The evaluation of vectors Q and Z is exploited using Eq. (17) and (18).

$$\vec{\mathbf{Q}} = 2\vec{\mathbf{l}}.\vec{\mathbf{r}} - \vec{\mathbf{l}} \tag{17}$$

$$\vec{Z} = 2\vec{r} \tag{18}$$

Here, the *l* value has a gradual decrease over the interval 2 to 0 (in exploitation and exploration phase) and *r* random vector is limited in the range of [0,1].

**Spiral Updating position:** The arithmetical evaluation of spiral equation on position update among the prey and humpback whale is explained by Eq. (19) and (20).

$$\mathbf{D} = \left| \mathbf{H}^*(\mathbf{t}) - \mathbf{H}(\mathbf{t}) \right| \tag{19}$$

$$H(t+1) = D'.e^{dz}.(\cos 2\pi q) + H^{*}(t)$$
(20)

In this, the logarithmic spiral's shape is given as d and is always constant, and the random number is expressed by q and is consistently shared within the interval -1 to 1.

Every encircling path imagines only 50% probability which can pursue the logarithmic path, if not the shrinking encircle mechanism during optimization. The arithmetical construction of evaluating the probability is depicted as per the Eq. (21), in this the every feasible encircling path is given by pb.

\_

$$H(t+1) = H^{*}(t) \quad Q.D \qquad \text{if } pb < 0.5$$

$$\vec{H}(t+1) = \vec{D}'.e^{dz}.(\cos 2\pi q) + \vec{H}^{*}(t) \quad \text{if } pb \ge 0.5$$
(21)

The global search is taken place by updating the search agent position by means of selected search agent in random, despite its dependence on the identified best search agent. If the Q random value poses a greater value than one, then this technique might be adopted. Eq. (22) and (23) portrays the arithmetical evaluation of this WOA principle.

Vol. 2 No.2 April 2019

Multimedia Research

$$\vec{\mathbf{D}} = \left| \vec{\mathbf{W}} \cdot \vec{\mathbf{H}}_{rad} - \vec{\mathbf{H}}(t) \right| \tag{22}$$

$$\vec{H}(t+1) = \vec{H}_{rad} - \vec{Q}.\vec{D}$$
(23)

In this,  $H_{rad}$  is elected in random from the whales at the present tryout run. The WOA algorithm's pseudo code is delineated in Algorithm 1.

Algorithm 1: Pseudo code of Whale Optimization algorithm
Initiate the whale population $H_i$ (i = 1,2,,n)
Evaluate the fitness of every search agent
$H^*$ = best search agent
While (t < maxiteration)
For every search agent
Update 1,Q,D,q and <i>pb</i>
if (pb < 0.5)
$if( \mathbf{Q}  < 1)$
Update the present search agent position by Eq. (15)
Else if $( \mathbf{Q}  \ge 1)$
Choose the random search agent $(H_{rand})$
Update the present search agent position by Eq. (23)
End if
Else if $(pb \ge 0.5)$
Update the current search position by Eq. (20)
End if
End for
Verify if any search agent leave afar the search space and modify it
Estimate the fitness of every search agent
Update $H^*$ as per the best solution
t = t + 1
End while
$\operatorname{return}\operatorname{H}^{*}$

## **5 Results and Discussions**

#### 5.1 Dataset description

The simulation experiment of the implemented image forgery detection was made by a software tool named MATLAB and the results were analyzed.

#### 5.2 Description on the dataset

Two datasets are implemented for the experiment purpose namely DSO-1 and DSI-1.

(i) DSO-1 (dataset 1): In this, the image resolution of  $2048 \times 1536$  pixels is used with 200 indoor and outdoor images. This dataset is involved with 100 forged images and 100 original images. The forgery of the image is made by using more than one individual in the source image with more than one person.

(ii) DSI-1 (dataset 2): This involves 50 images having 25 original and 25 forged and that is acquired from diverse websites on the Internet having diverse resolutions.

#### 5.3 Comparative Analysis of dataset 1

Fig. 3 depicts the analysis on comparison over the proposed and conventional models for dataset 1. The performance of the implemented model is viewed under measures like Accuracy, Sensitivity, and Specificity. On considering the accuracy measure at learning percentage 0.9, the implemented model has a performance that is 45.94%, 35.45%, 3.45% better from kNN, NN and SVM, respectively. Similarly, for Sensitivity measure at learning percentage 0.5, the performance of the developed model has attained a superior solution than kNN, NN and SVM by 45.12%, 76.09%, and 22.68%, respectively. Further, in terms of Specificity at learning percentage 0.7, the introduced method is 49.51%, 17% and 21.35%

superior to kNN, NN and SVM, respectively. Therefore, the obtained results have shown the betterment of the implemented model over the other conventional models regarding certain measures.



Fig 3. Comparitive Analysis of the Proposed and Conventional model for dataset 1 regarding (a) Accuracy (b) Sensitivity and (c) Specificity

#### 5.4 Comparative Analysis of dataset 2

The comparative analysis of the proposed and traditional models for dataset 2 is symbolized in fig. 4. Here also, the performance is compared regarding certain measures. The result has explained that the performance of the introduced model is 54.92%, 41.26%, and 18.18% better from kNN, NN and SVM, respectively in terms of accuracy at learning percentage 0.5. While taking the Sensitivity measure, the implanted model has better performance and that is 64%, 48% and 36.43% than kNN, NN and SVM, respectively. Likewise, the implemented model in terms of specificity at learning percentage 0.9 has gained superior solution over kNN, NN and SVM by 0.99%, 3.63%, and 1.86%, respectively. The result has thus revealed the improvement of the proposed model.



Fig 4. Comparative Analysis of the Proposed and Conventional model for dataset 2 regarding (a) Accuracy (b) Sensitivity and (c) Specificity

## **6** Conclusion

This framework has introduced a new automatic image forgery detection method under four stages (i) Illumination map computation, (ii) Face detection, (iii) Feature extraction, and (iv) Classification. The first phase has processed as illumination map estimation, which contains two processes gray world estimates and inverse-Intensity chromaticity. The next was the face detection stage, where the face can be detected by applying the Viola-Jones algorithm. The feature extraction is the subsequent phase that uses GLCM for extracting the facial features. In classification, the NN has been deployed to classify the extracted features. The optimization was the final tactic in this paper, where the NN's weight has been optimally selected by means of the WOA algorithm. Finally, the performance of the implanted model was distinguished with conventional models and the result was analyzed. On considering the accuracy measure at learning percentage 0.9, the implemented model has a performance that was 45.94%, 35.45%, 3.45% better from kNN, NN and SVM, respectively.

# **Compliance with Ethical Standards**

Conflicts of interest: Authors declared that they have no conflict of interest.

**Human participants:** The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

## References

- SundusFarooq, Muhammad HaroonYousaf, FawadHussain," A generic passive image forgery detection scheme using local binary pattern with rich models", Computers & Electrical Engineering, vol.62, pp.459-472, August 2017
- [2] Daniel CavalcantiJeronymo, Yuri Cassio CampbellBorges, Leandro dos SantosCoelho," Image forgery detection by semi-automatic wavelet soft-Thresholding with error level analysis", Expert Systems with Applications, vol. 85, pp.348-356, 1 November 2017
- [3] Rani SusanOommen, M.Jayamohan, S.Sruthy," Using Fractal Dimension and Singular Values for Image Forgery Detection and Localization", Proceedia Technology, vol.. 24, pp.1452-1459, 2016
- [4] C. Pun, X. Yuan and X. Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1705-1716, Aug. 2015.
- [5] O. Mayer and M. C. Stamm, "Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration," IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1762-1777, July 2018.
- [6] Felzenszwalb, P.F., Huttenlocher, D.P.: 'Efficient graph-based image segmentation', Int. J. Vis. Comput., 59, (2), pp. 167-181, 2004
- [7] Mathur, M.K., Bhati, P.: 'Face objects detection in still images using Viola– Jones algorithm through MATLAB tools', Int. J. Innov. Res. Comput. Commun. Eng., 5, (2), pp. 2468–2476, 2017
- [8] Chris EbeyHoneycutt, RoyPlotnick,"Image analysis techniques and gray-level co-occurrence matrices (GLCM) for calculating bioturbation indices and characterizing biogenic sedimentary structures", Computers & Geosciences, vol.34, no.11, pp.1461-1472, November 2008
- [9] Yogeswaran Mohan, Sia Seng Chee, Donica Kan Pei Xin and Lee Poh Foong, "Artificial Neural Network for Classification of Depressive and Normal in EEG, 2016 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES), 2016.
- [10] Seyedali Mirjalili and Andrew Lewis, "The Whale Optimization Algorithm", Advances in Engineering Software, vol. 95, pp.51–67, 2016.
- [11] R. Dixit, R. Naskar and S. Mishra, "Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD," IET Image Processing, vol. 11, no. 5, pp. 301-309, 5 2017.
- [12] R. Dixit and R. Naskar, "Review, analysis and parameterisation of techniques for copy-move forgery detection in digital images," IET Image Processing, vol. 11, no. 9, pp. 746-759, 9 2017.
- [13] H. Lin, J. Si and G. P. Abousleman, "Orthogonal Rotation-Invariant Moments for Digital Image Processing," IEEE Transactions on Image Processing, vol. 17, no. 3, pp. 272-282, March 2008.
- [14] Wu-Chih Hu, Wei-Hao Chen, Deng-Yuan Huang, Ching-Yu Yang," Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes", Multimedia Tools and Applications, vol.75, no.6, pp 3495–3516,March 2016.
- [15] Xin Wang, "Moving window-based double haar wavelet transform for image processing," IEEE Transactions on Image Processing, vol. 15, no. 9, pp. 2771-2779, Sept. 2006.
- [16] S. Ebrahimi, E. Angelini, L. Gajny and W. Skalli, "Lumbar spine posterior corner detection in X-rays using Haar-based features," 2016 IEEE 13th International Symposium on Biomedical Imaging (ISBI), Prague, 2016, pp. 180-183.
- [17] J. Jang and M. Cho, "Color Artifact-Free Three-Dimensional Integral Imaging Display with Large Depth Using a Lens Array Based on Sublens Structure," Journal of Display Technology, vol. 12, no. 6, pp. 610-615, June 2016.
- [18] S. Wu and H. Nagahashi, "Parameterized AdaBoost: Introducing a Parameter to Speed Up the Training of Real AdaBoost," IEEE Signal Processing Letters, vol. 21, no. 6, pp. 687-691, June 2014.
- [19] L. Cuimei, Q. Zhiliang, J. Nan and W. Jianhua, "Human face detection algorithm via Haar cascade classifier combined with three additional classifiers," 2017 13th IEEE International Conference on Electronic Measurement & Instruments (ICEMI), Yangzhou, 2017, pp. 483-487.
- [20] V. Gaike, N. Akhter, K. V. Kale and P. Deshmukh, "Application of higher order GLCM features on mammograms," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, 2015, pp. 1-3.