Vol.3 No.1 Jan 2020

Multimedia Research

Received 2 October, Revised 18 November, Accepted 26 December

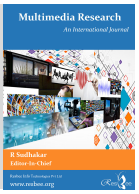

Image Forgery Detection Using Back Propagation Neural Network Model and Particle Swarm Optimization Algorithm

Cristin R
Department of Computer Science Engineering,
GMR Institute of Technology,
Rajam, Andhra Pradesh, India
rcristin2015@gmail.com

Gladiss Merlin N.R
Jeppiaar Institute of Technology,
chennai, Tamil Nadu, India

Ramanathan L
School of Computer Science & Engineering,
Vellore Institute of Technology,
Vellore, Tamil Nadu, India

Vimala S
Department of Electronics and Communication Engineering,
Prathyusha Engineering College,
Tiruvallur, Tamil Nadu India

Abstract: From the images, forgery detection is ahead noteworthy attention as there are numerous editing tools that facilitate to form the edition by means of removal or objects manipulation from the images. These editing tools not at all abscond any forgery trace as a result, growing the challenges of the system to identify the existence of the manipulations. Accordingly, this work presents a new forgery recognition approach which is on the basis of the supervised learning algorithm. This algorithm is presented concerning exploiting the BPNN and optimization is set up by exploiting the Particle Swarm Optimization (PSO) algorithm. The classification is done by exploiting the proposed classifier exploits the texture features attained from the GWTM descriptor so that the features are attained from the face-detected images retrieved by exploiting the Viola-Jones approach. By utilizing two datasets, the simulation is performed to show the efficiency of the proposed model. By utilizing the datasets the analysis shows that the proposed model obtained superior performance while evaluating with few conventional forgery detection systems.

Keywords: Forgery Detection; Viola Jones; GWTM; BPNN; PSO

Nomenclature

Abbreviations	Descriptions
SAE	Stacked Auto-Encoders
FrZMs	Fractional Zernike Moments
LCA	Lateral Chromatic Aberration
SVM	Support Vector Machine
CNN	Convolutional Neural Networks
HSV	Huesaturation- Value
R-CNN	Refined CNN
QPCETMs	Quaternion Polar Complex Exponential Transform Moments
KNN	K-Nearest Neighbors
FrQZMs	Fractional Quaternion Zernike Moments
LSTM	Long-Short Term Memory
FAR	False Alarm Rate
C-CNN	Coarse CNN
NN	Neural Network
OF	Optical Flow
RMSE	Root Mean Square Error
C2RNet	Coarse-To-Refined Network
BPNN	Back Propagation Neural Network

1. Introduction

The image forgery detection has to turn out to be extremely complex as exploited images are frequently visually impossible to differentiate from real images [1]. In numerous techniques, a manipulated image with the introduction of advanced editing image tools. The categorization of image manipulation has the ability to categorize into two groups such as content-changing and content-preserving. The initial

https://doi.org/10.46253/j.mr.v3i1.a3

categorization of manipulation, for instance: blur, compression, and contrast enhancement happens mostly because of the post-processing, and they are taken into consideration as minimum detrimental as they do not alter any semantic content. The latter categorization such as object removal, copy-move, and splicing, image content is reshaped randomly and changes the meaning of the semantic considerably. The manipulations of content-altering are expressed as fake or deceptive information. Since the quantity of tampered images produces during a rate of massive, it turns out to be vital to recognize the image manipulation to avert viewers from being obtainable by means of deceptive information. In recent times, from a video or image, the content-changing manipulation detection has to turn out to be a region of rising interest in miscellaneous scientific and surveillance/security technologies.

Generally, digital forensic methods are categorized into active and passive else blind methods. Moreover, 2 common active forensic applications are digital signatures and watermarking, these two applications are embedded definite substantiation data in visual media of their manufacture; however, these approaches need particular hardware, preventive technologies. The blind or passive forensic methods confirm the authenticity by searching features of intrinsic in the media remnants using manipulation acts or attainment devices, in the absence of exploiting some pre-embedded signals. Moreover, it is a novel investigate field rising in the previous decade, and it was shown the potential tool for digital visual media in the authentication field.

Digital multimedia forensics has revealed the features of statistical, which is intrinsic to images, which is exploited to recognize changed images [9]. A significant category of modification is to identify the copy-paste forgery image, wherever image content from one image is copied and pasted into another, else similar, image. This process is frequently performed to maliciously alter significance or image context using concealing or inserting objects in it. The previous study possesses exhibited the copy-paste forgeries is recognized by discovering localized discrepancy in features of the intrinsic image like resampling traces [10] contrast enhancement [12], JPEG compression [11], sensor noise [15] and median filtering [13]. In addition, methods which process using discovering duplicate blocks image [16] and by corresponding SIFT features [17] had utilized to identify copy-move forgeries image, whereas the content of the image is pasted into the similar image. Research in [18] presents a statistical construction of such forgery detection features for the fusion.

The majority of the modern classification of image tampering methods uses the characteristics of the frequency domain and/or image statistical properties. By multiple JPEG compressions, the analysis of the artifacts is besides used in [10], to identify manipulated images that are appropriate merely to the formats of JPEG. In [12], the noise was presented to the compressed JPEG image to enhance the resampling recognition analysis. Deep learning shows potential performance in diverse visual detection tasks like scene classification, detection of an object, and semantic segmentation in computer vision. A few latest deep learning-based approaches like CNN and SAE was also used to classify/detect image manipulations. The majority of the conventional forgery recognition methods concentrate on recognizing an exact tampering method, like copy-move and splicing in media forensics. Hence, a single method may not succeed in other categories of tampering.

The main objective of the work is to propose a PSO-BPNN algorithm. The proposed approach is the PSO-BPNN classifier which utilizes the PSO algorithm to train the BPNN so that the images are classified on the basis of the availability of the forgery.

2. Literature Review

In 2018, Owen Mayer et al [1] proposed a novel method to identify forged image areas that were on the basis of identifying localized LCA discrepancy. Hence, an analysis method that detains inconsistency among global and local calculates of LCA was proposed. Moreover, this approach was used to create forgery recognition like a hypothesis analysis issue and a recognition statistic that was derived, that an optimal method was exhibited while definite circumstances were met. Moreover, a novel and competent LCA estimation approach were presented. To achieve a block matching algorithm was proposed, named diamond search that competently estimates the LCA in a localized area.

In 2018, Yuanman Li and Jiantao Zhou [2], developed a rapid and effectual copy-move forgery recognition method during hierarchical matching of feature points. Initially, to produce an adequate number of key points were exhibit which subsists still in diminutive or smooth areas, by worsening the rescaling and contrast threshold the input image. Subsequently, a new hierarchical matching approach was developed to resolve the keypoint matching issues in excess of an enormous number of key points. To minimize the FAR and precisely localize the tampered regions, a new iterative localization approach was presented by using the robustness properties and the color information for every key point.

In 2018, BEIJING CHEN et al [3] developed FrZMs for complex signals that were widespread to FrQZMs via quaternion algebra for quaternion signal processing in a holistic way. Initially, the

description of FrQZMs was developed and a proficient accomplishment technique to speed up the calculation of FrQZMs via FrZMs of every module of the quaternion signal.

In 2018, Khalid M. Hosny et al [4], presented techniques, which comprise a small number of steps. The input colored images were transformed into the HSV color model. Subsequently, by exploiting the Sobel operator, in the forged image, the edges of all objects were recognized. A morphological median filter and opening operator were exploited in eradicating redundant little objects. The duplicated objects' boundaries were precisely recognized.

In 2019, Jawadul H. Bappy et al [5], developed a maximum-confidence localization manipulation model that exploits LSTM cells, resampling features, an encoder-decoder network was exploited from non-manipulated ones to segment out manipulated areas. Features of resampling were exploited to detain artifacts like loss of JPEG quality, downsampling, rotation, shearing, and upsampling. To evaluate the discriminative characteristics among non-manipulated and manipulated areas the developed network exploits higher frequency domain and receptive field's correlation by integrating LSTM and encoder networks.

In 2018, SHAN JIA et al [6], developed a new technique for recognition of frame copy-move forgeries considering the 3 needs. A coarse-to-fine recognition scheme due to the OF and stable parameters were modeled. Especially analyzes of coarse recognition OF sum reliability to discover alleged tampered points. Subsequently, fine recognition experimented for the forgery exact position, and pairs of duplicated frame matching due to the OF correlation, and substantiation verifies to promote minimize the false detections.

In 2019, Bin Xiao et al [7], developed a splicing forgery recognition algorithm with 2 segments such as a C2RNet CNN and adaptive diluted clustering. The developed C2RNet cascades a C-CNN and an R-CNN and extracts the differences in the image properties among tampered and un-tampered areas with different scales from image patches.

In 2017, Victor Schetinger et al [8], worked on the image composition field was continually attempting to enhance the traditions in that an image can be improved and changed. Basically, when this was performed in the name of practicality and aesthetics, additionally it offers tools that were exploited to maliciously image modification. In this case, the digital image forensics field had to be organized to the pact by means of the arrival of the latest applications.

3. Proposed Model for Forgery Detection

The requirement for the automatic forgery recognition method happens in the current case, whereas image reliability is not guaranteed. The accessibility of a great quantity of comprehensible software facilitates manipulation and image editing which influences the originality of the image foremost to the illegitimate forgery. This work develops a forgery recognition method by exploiting proposed PSO-BPNN classification. For classification, the features are proposed and by exploiting the GWTM the extraction of features is done. At first, to the illumination map, the image is given by exploiting two estimations. In the next step, the Viola-Jones approach is used to recognize the faces in the image and subsequently, at last, the detection of the face images is given to the extraction of features by exploiting GWTM. To the SVNN classifier in order to form the three inputs, GWTM proposes 3 features that are concatenated that classify the features and it offers the information if it is non-forgery else forgery image. The schematic illustration of the proposed model is shown in Fig 1. In the database let I is an image, the image is given to recognize the forgery by exploiting proposed classifiers.

3.1 Estimation of Illumination Map

In this section, the evaluation of the illumination map [19] is shown. From the input image, the segments of superpixels are produced by exploiting the Huttenlocher and Felzenszwalb [20]. For all the individual superpixels the illumination color is estimated. To evaluate the illumination, the color estimators used such as estimation of the gray world and the chromaticity space of inverse-intensity.

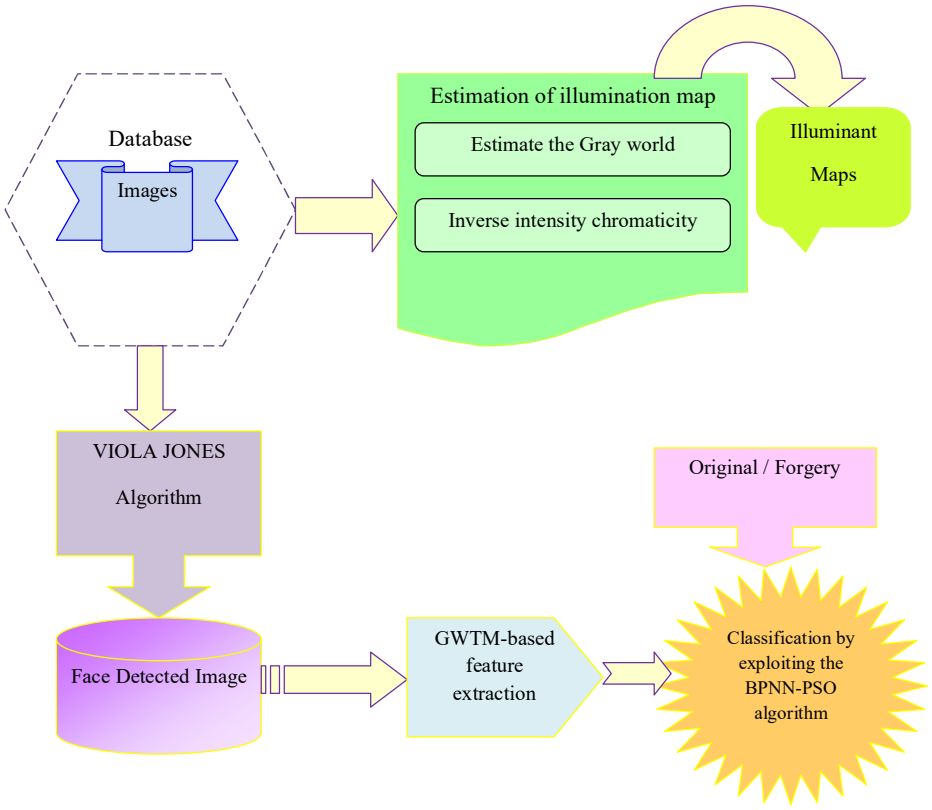

Fig. 1. *Schematic illustration of the adopted methodology for forgery detection exploiting the BPNN-PSO model*

i) Estimation of Gray world

In [21], gray is the average scene color therefore, from the average gray it is obvious that any divergence is the reason for illumination. Assuming that the RGB color as a pixel centered at x is indicated as eq. (1),

$$F(x)=[F_R(x),F_G(z),F_B(x)] \tag{1}$$

Consider an assumption, which needs to be an accurately diffuse reflection and the response of linear camera which are stated below.

$$F(x)=\int_{\psi} e(\delta,x)\,r(\delta,x)\,L(\delta)\,d\delta \tag{2}$$

In eq. (2), ψ indicates the visible light spectrum, $F_G(z)$ indicates the surface reflectance, δ indicates the light wavelength, $e(\delta,x)$ indicates the illuminant spectrum. The camera sensitivity to color is represented as, $L(\delta)$. The world gray hypothesis is extended by exploiting the manipulation of 3 parameters, such as the derivative order p, parameter of smoothing, ζ and Minkowski norm τ. The color of the illuminant e is stated in eq. (3).

$$K\,e^{p,\tau,\zeta}=\left(\int\left|\frac{\partial^p F^{\xi}(x)}{\partial x^p}\right|^{\tau}dx\right)^{\frac{1}{\tau}} \tag{3}$$

In eq. (3), K indicates the scaling factor, x indicates the pixel coordinate, $|\cdot|$ indicates the value of absolute. ∂ indicates the differentiation and $F^{\xi}(x)$ indicates the observed intensities at a location x which is smoothened by exploiting kernel ξ. For the color channel, the parameter e is calculated individually and the derivative operator enhances the robustness.

ii) Inverse-intensity chromaticity

Conversely, the estimation of the gray world, the assumption has done in this method shows the specular reflectance and diffuses. Assume the eq. (1) exhibits the RGB image pixel. The function is model as stated in eq. (4).

$$F(x)=[F_R(x),F_G(x),F_B(x)]^T \tag{4}$$

The connection among the function $F(x)$, the color channel chromaticity $\gamma_L(x)$, and illuminated channel chromaticity χ_L is stated as eq. (5).

$$\gamma_L(x) = n(x) \times \frac{1}{\sum_{j \in \{R,G,B\}} F_j(x)} + \vartheta_L \tag{5}$$

The function $n(x)$ indicates the geometric influences that cannot be computed methodically, however, experience an estimated solution. Hence, the only method of deciding the illuminant color is via the y-intercept ϑ_L which is decided using the pixels evaluation.

3.2 Map Viola-Jones for Face Extraction

The significance of exploiting the Viola-Jones approach [22] in order to detect the face is that the approach is competent and rapid in recognizing the face, and the computational speed, is stated in milliseconds. At first, from white pixels, the black pixels are marked and subtracted and the outcomes are evaluated by means of the value of threshold which the features are recognized on the basis of condition. The Viola-Jones steps are stated as below:

i) Haar-like features: It determines white and black segments of an image which exploits a rectangle around the face.

ii) Integral image formation: It is created by summing the individual pixels value with its neighbors' pixel values. Conversely, the individual pixel value is created by summing the neighboring pixel value 4 pixels that are gathered in the rectangle.

iii) Adaboost machine learning approach: It is the machine-learning algorithm used in order to detect the face and it pursues bagging model. The significance of the Adaboost method is to select small features in the face so that computation turns out to be simple and rapid. Moreover, it presents extremely important features by abandoning superfluous background.

iv)Concatenating features using Cascade classifier: It consists of a quantity of the classifiers which permits chosen of the face image. To the classifiers, every sub-window is transmitted so that to establish if the sub-window has face or not.

Hence, the Viola-Jones approach is used to recognize a face from the image is done effectively by exploiting aforesaid steps. By exploiting the Viola-Jones, the original image is used to detect the face.

3.3 Exploiting GWTM for Feature Extraction

By exploiting the GWTM operator, the input face-recognized images are given for the extraction of features [23]. The images are given to Gabor filter and wavelet transform, between that the wavelet images are created by exploiting the features and a wavelet transform on the basis of frequency and the orientation, which are decided by exploiting the Gabor filters. From the Gabor filter and the wavelet transforms, the output is subjected to the LBP method by means of the input image. For the input image, the evaluation of texture is evaluated which alters the input image into an array. From the LBP the output is fed to the analysis of histogram so that histogram produces the global image model.

In the GWTM operator, the Gabor filters and wavelet alters are beneficial, which is exploited to the extraction of the feature as they protect facial features. The GWTM regarded as the coefficient of approximation in order to extract the features as they have the inclination to disclose the features of facial on a dissimilar scale. In addition, Gabor filters produce the information of frequency and protect spatial and information of frequency for the image. The Gabor filters have a stage and the information of magnitude and image magnitude increases consequence as they protect the information of the edge efficiently.

i) Wavelet transforms

In the wavelet transforms, face recognized images are given which facilitate the evaluation of non-stationary and stationary images. The image into a set of functions is decomposed by the wavelet transform, called wavelets. The wavelet transform improves the accuracy of the forgery recognition procedure and the 2-dimensional wavelet transform and it is stated as follow:

$$T^h(u,v) = \frac{1}{\sqrt{UV}} \sum_{u=1}^{U-1} \sum_{v=1}^{V-1} I^h(u,v) * \sigma_{k,l}(u,v) \tag{6}$$

In eq. (6), $I^h(u,v)$ indicates the high-resolution input image and $\sigma_{k,l}(u,v)$ signifies the scaling function.

ii) Gabor filters

The Gabor filter is a subsequent phase of GWTM [14] and the intention of exploiting Gabor filtering in which Gabor filters terminate spatial orientation, area, and identifies the face edge recognized image. In addition, Gabor filters offer texture features and it is stated in eq. (7).

$$Y_{k,l}^{h}(sp)=\frac{\left\|D_{k,l}\right\|^{2}}{\varepsilon^{2}}\times e^{\left(-\frac{\left(\left\|D_{k,l}\right\|^{2}-\left\|sp\right\|^{2}\right)}{2\varepsilon^{2}}\right)}\left[e^{u,D_{k,l}sp}-e^{-\frac{\varepsilon^{2}}{2}}\right] \tag{7}$$

In eq. (7), l and k indicates the scale and orientation of the Gabor filters and sp indicates the spatial position. $D_{k,l}$ is exploited to decide the value of the magnitude is represented in eq. (8).

$$D_{k,l}=\frac{D_{max}}{\varpi} \tag{8}$$

In eq. (8), ϖ indicates the ratio of frequency. The output of the Gabor filter is face recognized image convolution $I^{h}(u,v)$ and $X_{u,v}^{h}(sp)$, as stated in eq. (9),

$$g_{k,l}^{h}(u,v)=I^{h}(u,v)*X_{u,v}^{h}(sp) \tag{9}$$

The output of the Gabor filter complex form is indicated in the eq. (10) which is used to recognize the image forgery.

$$g_{k,l}^{h}(u,v)=M_{k,l}(u,v)\times e^{i\phi(u,v)} \tag{10}$$

On the basis of the obtainable frequency channels and directions, from face detected image, the local features can be extracted from the Gabor filter. From the Gabor filters, the image features are attained via magnitude, Gabor phase features, imaginary and real Gabor features. Here, the additional procedures are preceded by exploiting the real part of the Gabor magnitude.

iii) Utilizing LBP for local features extraction

From the Gabor features and the wavelet, the output is used to LBP in order to extract the local features. The gray level image is considered as the input to the LBP so that the LBP pattern does not alter on the basis of alters in the monotonic grayscale image. The center pixel is fixed as, t_c and subsequently, evaluation is done among neighboring pixels and center pixels from the input gray image.

$$LBP(p_c,q_c)=\sum_{i=0}^{7}Q(t_i-t_c)\times 2^{i} \tag{11}$$

$$Q(b)=\begin{cases}1 & ;\ b\geq 0\\ 0 & ;\ b<0\end{cases} \tag{12}$$

In eq. (11), t_i refers to the neighboring pixel to the center pixel t_c. While pixel value of the neighboring pixel is higher than center pixel during comparison, the neighboring pixel increases the value '1' or else; the value of the pixel becomes '0' as stated in the eq. (12). Hence, a novel image with '1's and '0's is produced and it is exploited as the threshold image and LBP pattern is created by changing the threshold of the binary image into the equivalent decimal value. The classification of texture is performed by exploiting input face recognized an image, estimate wavelet transform coefficients, and the Gabor magnitude real part. Eq. (13) states operator of LBP for coefficients of approximation.

$$T_{LBT}^{h}(u,v)=LBP\left[T^{h}(u,v)\right] \tag{13}$$

In eq. (13), $T^{h}(u,v)$ signifies the wavelet transform output and $T_{LBT}^{h}(u,v)$ signifies the wavelet transform LBP. Using the face recognized image to the LBP is stated in eq. (14).

$$I_{LBP}^{h}(u,v)=LBP\left[I^{h}(u,v)\right] \tag{14}$$

In eq. (14), $I_{LBP}^{h}(u,v)$ signifies the HR image LBP. The Gabor filter LBP output is stated in eq. (15).

$$g_{LBP}^{h}(u,v)=LBP\left[g_{k,l}^{h}(u,v)\right] \tag{15}$$

In eq. (15), $g_{k,l}^{h}(u,v)$ signifies filter output of the Gabor from the HR images and the Gabor filter LBP output it is stated $g_{LBP}^{h}(u,v)$.

iv)Representation of histogram

In the image, the histogram shows the input image pixel values and the image illustration signifies the frequency of the gray level. The input to histogram indication represents outcomes of Gabor filter, wavelet transform, and face recognized image. The histogram consequence is indicated in eq. (16).

$$f_1^{FACE} = \left\{ HT_1^1 \middle\| HT_1^2 \middle\| HT_1^3 \right\} \tag{16}$$

In eq. (16), HT_1^1 indicates the output of histogram equivalent to wavelet transform for the face recognized image1, HT_1^2 indicates the histogram output for Gabor filter consequence of face recognized image1, and HT_1^3 indicates the histogram output for the input face recognized image1. f_1^{FACE} indicates the GWTM feature of face- recognized image 1. In LBP histogram, while there subsist 256 bins subsequently, the GWTM feature-length is 768. If there are 3 faces in image subsequently, features of GWTM are stated as below:

$$f_2^{FACE} = \left\{ HT_2^1 \middle\| HT_2^2 \middle\| HT_2^3 \right\} \tag{17}$$

$$f_3^{FACE} = \left\{ HT_3^1 \middle\| HT_3^2 \middle\| HT_3^3 \right\} \tag{18}$$

In eq. (17) and (18), f_2^{FACE} and f_3^{FACE} symbolizes GWTM features of face recognized image two and three, correspondingly. HT_2^1, HT_2^2, and HT_2^3 indicates the outputs of histogram similar to the Gabor filter, wavelet transform, and face recognized input image 2. HT_3^1, HT_3^2, and HT_3^3 represents the histogram outputs of the face recognized image 3 which symbolizes Gabor filter, wavelet transform, and the face recognized input image 3.

3.4 Exploiting Adopted Classifier Feature Input for Classification

The feature vector attained because of feature extraction by exploiting the GWTM is $f_t^{FACE} = \left\{ f_1^{FACE}, ..., f_u^{FACE}, ..., f_t^{FACE} \right\}$. Every feature is of dimension, (1×768) and features are adopted to the proposed classifier in order to classify the image. The prime feature to the proposed classifier is produced by concatenating GWTM features, f_1^{FACE} and f_2^{FACE}, to produce,

$$f_1^* = \left[f_1^{FACE} \middle\| f_2^{FACE} \right] \tag{19}$$

The subsequent input to the proposed classifier is produced by amalgamation of features f_2^{FACE} and f_3^{FACE} is stated in eq. (20).

$$f_2^* = \left[f_2^{FACE} \middle\| f_3^{FACE} \right] \tag{20}$$

The third feature vector subjected to classifier input that is attained by concatenating features f_3^{FACE} and f_1^{FACE}, it is shown as follows:

$$f_3^* = \left[f_3^{FACE} \middle\| f_1^{FACE} \right] \tag{21}$$

Generally, the feature concatenation is stated in eq. (22).

$$f_a^* = \left[f_u^{FACE} \middle\| f_v^{FACE} \right]; \forall u \,\&\, v; 0 \le a \le b \tag{22}$$

In eq. (22), b indicates the total number of the probable training vectors produced by exploiting the GWTM features of the face detected images. From p^{th} and the q^{th} face detected images, f_p^{FACE} and f_q^{FACE} are the GWTM features extracted. Hence, the training feature vector exploited as input to the proposed classifier is stated in eq. (23).

$$f^* = \left\{ f_1^*, f_2^*, f_3^*, ..., f_a^* \right\} \tag{23}$$

4. Proposed BPNN-PSO Algorithm for the Classification Image

The BPNN is trained to exploit the PSO. The significance of the proposed method is that the calculational speed is superior and the optimal solution converges to the global optimal solution. The procedures of alteration to code format are easy and straightforward whilst utilizing minimum time.

4.1 Back Propagation Neural Network Model

In engineering applications, generally, Back Propagation Neural Network (BPNN) is the well-liked NN algorithm. It was established that the performance of the BPNN algorithm has a superior prediction. Generally, BPNN is considered as a kind of feedforward NN. It appends a backward propagation method to model the feedforward NN. It comprises an input, output and a hidden layer. By weight, the input layer obtains the input signals and transmits the processed signal to the hidden layer. Here, the inner

processing layer is considered as the hidden layer is that suggests the information and it is classified as single and multiple hidden layers [24].

In the input layer, the output from a neuron is stated as below:

$$OP_{mn} = I_{mn}, m = 1,2,....,N, \quad n = 1,2,.....l \tag{24}$$

In the hidden layer, the output from a neuron is stated as below:

$$OP_{mn} = f\left(\sum_{n=0}^{l} CW_n OP_{mn}\right), \quad n = 1,2,.....k \tag{25}$$

In the output layer, the output from a neuron is stated as below:

$$X_m = f\left(\sum_{p=0}^{k} CW_p OP_{mp}\right), \quad p = 1,2,.....k \tag{26}$$

In eq. (24) k indicates the number of hidden neurons CW_p indicates the linked weight from p^{th} hidden neurons to the output neuron and CW_{pn} indicates the linked weight from the n^{th} input neuron to the p^{th} hidden neuron. Fig 2 shows the flow chart of the BPNN model.

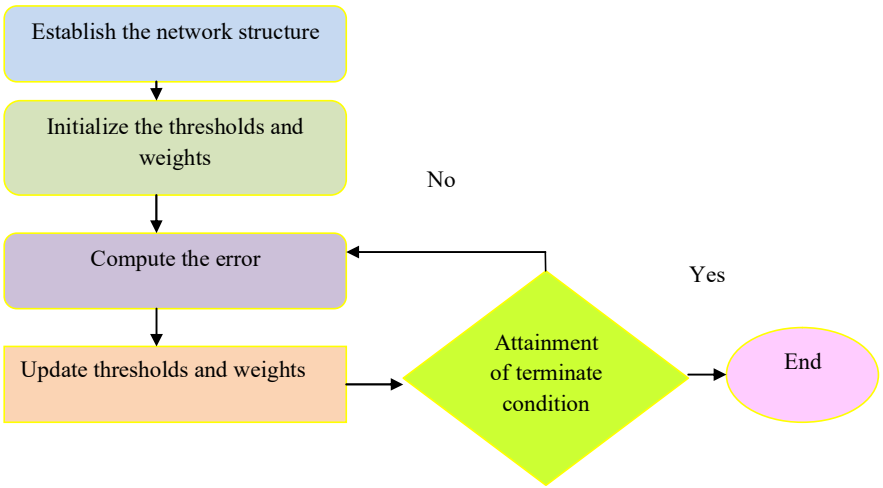

Fig. 2. *Flow chart of the BPNN model*

4.2 Particle Swarm Optimization Approach

In the PSO approach, every particle indicates a solution to the issue. The statistical nature of particles is a fitness value that signifies the fitness model. The speed, and location of every particle in space, is dissimilar, and the particle motion is affected by its adjacent particles [25]. Fig 3 demonstrates the flow diagram of the PSO technique is demonstrated. At first, the PSO approach initializes a collection of particles, by exploiting the speed, location, and fitness to explain the features of every particle [26]. While exploiting the PSO approach to optimize the BPNN technique, every particle indicates a set of thresholds and weights of BPNN. With the intention of the critic, each particle quality, the fitness model exploited is the RMSE of radionuclide release rate experimented using True Actual Rate and BPNN. If there are N sets of training data, subsequent for a set of thresholds and weights, equivalent fitness value is stated as below:

$$\text{Fit value} = \sqrt{\frac{1}{N}\sum_{t=1}^{N}(X_t - Op_t)^2} \tag{27}$$

Whilst the utmost iterations time is attained, the PSO technique is finished, and a population with the least fitness value can be attained and the population indicates the best solution to the issue.

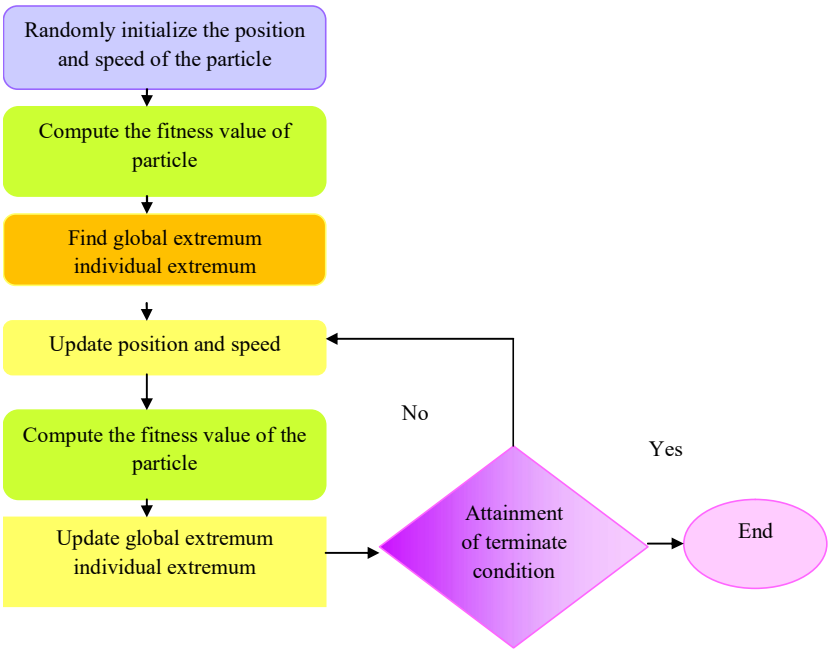

Fig. 3. *Flow chart of the PSO algorithm*

5. Results and Discussions

5.1 Simulation Setup

In this paper, the results of the proposed technique were shown to reveal the efficiency of the proposed algorithm. The simulation of the proposed algorithm to detect the forgery was performed in the system. The methods obtained for evaluation comprise the SVM, KNN, and NN, in order that evaluation was done with them to show the dominance of the proposed model.

For the simulation, two datasets [19], like DSI-1 as well as DSO-1, are used.

a) DSO-1: DSO-1 (dataset 1) comprises of 200 indoor and outdoor images with an image resolution of 2048x1536 pixels. The dataset consists of 100 forged images and 100 original images. The images are forged involving one or more individuals in the source image with one or more persons.

b) DSI-1: DSI-1 (dataset 2) comprises of 50 images with 25 original and 25 doctored images obtained from different websites in the Internet with different resolutions.

5.2 Performance Analysis

Fig. 4 exhibits the comparative analysis of the proposed technique for training percentage=0.9 in the DSO-I dataset for accuracy, specificity, and sensitivity. Fig. 5 exhibits the comparative analysis of the proposed technique for cross fold=10 in the DSO-I dataset.

Fig. 6 demonstrates the comparative analysis of the proposed technique for training percentage=0.9 in the DSI-I dataset for specificity, accuracy, and sensitivity. Fig. 7 reveals the comparative analysis of the proposed method for cross fold=10 in the DSI-I dataset.

The overall analysis shows that the proposed technique performance is superior to conventional methods like KNN, NN and SVM algorithms.

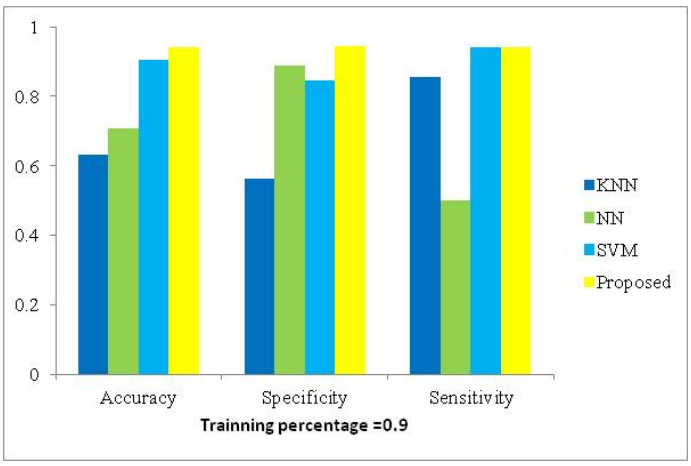

Fig. 4. *Comparative analysis of the proposed algorithm for training percentage=0.9 in DSO-1 Dataset*

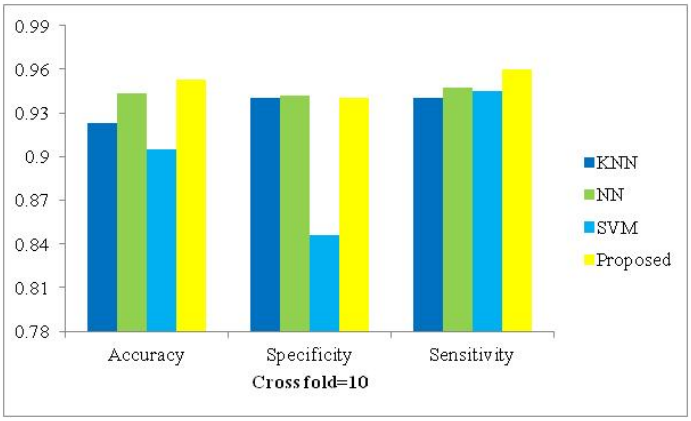

Fig. 5. *Comparative analysis of the proposed algorithm for cross fold =10 in DSO-1 Dataset*

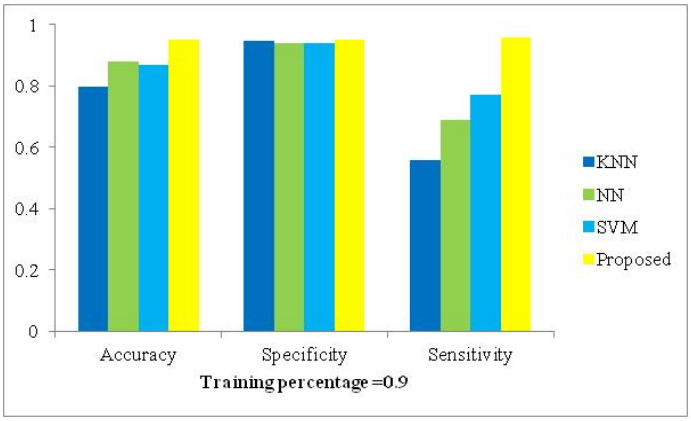

Fig. 6. *Comparative analysis of the proposed algorithm for training percentage =0.9 in DSI-1 Dataset*

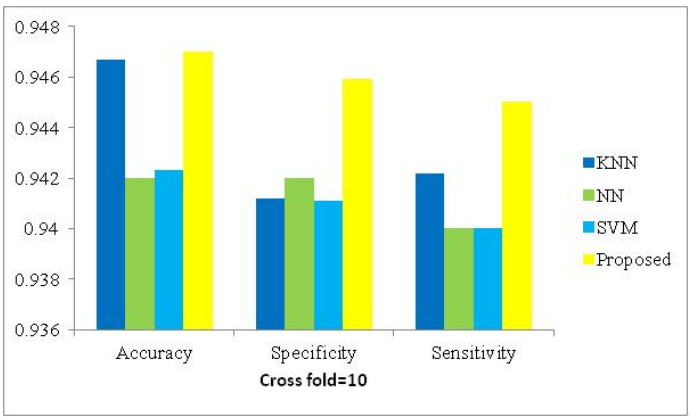

Fig. 7. *Comparative analysis of the proposed algorithm for cross fold =10 in DSI-1 Dataset*

5. Conclusion

The major aspire of this study was to concentrates on a method to recognize the forgery for that illumination-based texture descriptor and PSO-BPNN based classifier was utilized. The proposed PSO-BPNN classifier contributes to classifying the images as non-forged or forged images. The images were color altered in order to facilitate simple extraction of the feature and the altered image was used to the Viola-Jones approach that efficiently discovers the face in the image. By exploiting the GWTM the face recognized image was approved to the extraction of features and features were subjected to classifier for classification. The proposed classifier was established to be highly robust and effectual in recognizing forged images. The classifier was extremely effectual which presents improved classification accurateness and it was not computationally complex. Using the two datasets the simulation was done regarding the crossfold validation and the training percentage. The evaluation exploiting the datasets reveals that the proposed approach obtained better performance. In the images, to recognize the attendance of the forgery, the proposed model was extremely accurate.

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

[1] O. Mayer and M. C. Stamm, "Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration," IEEE Transactions on Information Forensics and Security, Volume. 13, issue. 7, page no. 1762-1777, July 2018.

[2] Y. Li and J. Zhou, "Fast and Effective Image Copy-Move Forgery Detection via Hierarchical Feature Point Matching," IEEE Transactions on Information Forensics and Security, Volume. 14, issue. 5, page no. 1307-1322, May 2019.

[3] B. Chen, M. Yu, Q. Su, H. J. Shim and Y. Shi, "Fractional Quaternion Zernike Moments for Robust Color Image Copy-Move Forgery Detection," IEEE Access, Volume. 6, page no. 56637-56646, 2018.

[4] K. M. Hosny, H. M. Hamza and N. A. Lashin, "Copy-for-duplication forgery detection in colour images using QPCETMs and sub-image approach," IET Image Processing, Volume. 13, issue. 9, page no. 1437-1446, 18 7 2019.

[5] J. H. Bappy, C. Simons, L. Nataraj, B. S. Manjunath and A. K. Roy-Chowdhury, "Hybrid LSTM and Encoder–Decoder Architecture for Detection of Image Forgeries," IEEE Transactions on Image Processing, Volume. 28, issue. 7, page no. 3286-3300, July 2019.

[6] S. Jia, Z. Xu, H. Wang, C. Feng and T. Wang, "Coarse-to-Fine Copy-Move Forgery Detection for Video Forensics," IEEE Access, Volume. 6, page no. 25323-25335, 2018.

[7] Bin Xiao, Yang Wei, Xiuli Bi, Weisheng Li, Jianfeng Ma," Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering", Information Sciences, Volume 511, page no 172-191, February 2020.

[8] Victor Schetinger, Massimo Iuliani, Alessandro Piva, Manuel M. Oliveira,"Image forgery detection confronts image composition",Computers & Graphics, Volume 68, page no 152-163, November 2017,.

[9] M. C. Stamm, M. Wu, and K. J. R. Liu, "Information forensics: An overview of the first decade," Access, IEEE, Volume. 1, page no. 167–200, 2013.

[10] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," Signal Processing, IEEE Transactions on, Volume. 53, no. 2, page no. 758–767, 2005.

[11] H. Farid, "Exposing digital forgeries from JPEG ghosts," Information Forensics and Security, IEEE Transactions on, Volume. 4, issue. 1, page no. 154–160, 2009.

[12] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," Information Forensics and Security, IEEE Transactions on, Volume. 5, issue. 3, page no. 492–506, 2010.

[13] M. Kirchner and J. Fridrich, "On detection of median filtering in digital images," in IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics, page no. 754 110–754 110, 2010.

[14] X. Kang, M. C. Stamm, A. Peng, and K. J. R. Liu, "Robust median filtering forensics using an autoregressive model," IEEE Transactions on Information Forensics and Security, Volume. 8, issue. 9, page no. 1456–1468, 2013.

[15] M. Chen, J. Fridrich, J. Luk´aˇs, and M. Goljan, "Imaging sensor noise as digital x-ray for revealing forgeries," in Proceedings of the 9th International Conference on Information Hiding. Springer-Verlag, pp. 342–358, 2007.

[16] J. Fridrich, D. Soukal, and J. Luk´aˇs, "Detection of copy-move forgery in digital images," in in Proceedings of Digital Forensic Research Workshop. Citeseer, 2003.

[17] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFTbased forensic method for copy–move attack detection and transformation recovery," Information Forensics and Security, IEEE Transactions on, Volume. 6, Issue. 3, page no. 1099–1110, 2011.

[18] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFTbased forensic method for copy–move attack detection and transformation recovery," Information Forensics and Security, IEEE Transactions on, Volume. 6, Issue. 3, page no. 1099–1110, 2011.

[19] Tiago José de Carvalho; Christian Riess; Elli Angelopoulou; Hélio Pedrini; Anderson de Rezende Rocha, "Exposing Digital Image Forgeries by Illumination Color Classification", IEEE Transactions on Information Forensics and Security, Volume.8, Issue.9, pp.1182 - 1194, 2013.

[20] P. F. Felzenszwalb and D. P. Huttenlocher, "Efficient graph-based image segmentation ", International Journal of Visual Computing, Volume.59, Issue.2, page no. 167–181, 2004.

[21] G. Buchsbaum, "A spatial processor model for color perception," Journal of Franklin Institute, Volume. 310, Issue. 1, page no. 1–26, Jul. 1980.

[22] Mridul Kumar Mathur and Priyanka Bhati, "Face Objects Detection in still images using Viola-Jones Algorithm through MATLAB TOOLS" , International Journal of Innovative Research in Computer and Communication Engineering, Volume.5, Issue.1, February 2017.

[23] Renjith Thomas & M. J. S. Rangachar, "Integrating GWTM and BAT algorithm for face recognition in low-resolution images", The Imaging Science Journal, Volume. 64, Issue. 8, 2016.

[24] Yan L, Hu P, Li C, Yao Y, Xing L, Lei F, et al. The performance prediction of ground source heat pump system based on monitoring data and data mining technology. Energy Build; volume 127: page no. 1085–95, 2016.

[25] J. Zhang, S. Member, A.C. Sanderson, JADE: Adaptive Differential Evolution with Optional External Archive, volume 13, page no 945-958, 2009.

[26] Xiwen Cai, Liang Gao, Fan Li,"Sequential approximation optimization assisted particle swarm optimization for expensive problems", Applied Soft Computing, Volume 83, October 2019.