Received: November 21, 2017

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Novel Method of Scale-Invariant Feature Transform Based Image Forgery Detection

Enumula Mahesh[1*] Suman Maloji[1] Dhyapulai Nagendra Rao[2]

[1]*Koneru Lakshmaiah University, India*
[2]*Dasari Rama Kotaiah Institute of Science and Technology, India*
* Corresponding author's Email: emaheshphd2017@gmail.com

Abstract: Now a days Image forgery (IF) makes many problems in a society. Super Pixels Segmentation and Scale-Invariant Feature Transform based Image Forgery Detection (SPS-SIFT-IFD) has introduced to detect the forgeries in the images. The forgery region extraction algorithm replaces the features point with small SP as feature blocks and neighboring blocks that have similar local color features has been identified by the Scale-Invariant Feature Transform (SIFT) technique. Artificial Neural Network (ANN) classifier is used for better detection of forged parts in the original images. It applies the morphological operation to the merged regions to generate the detected forgery regions. The experimental results indicate that the SPS-SIFT-IFD scheme achieve much better detection results even under various challenging conditions compared with the existing Forgery Detection (FD) methods. Finally, SPS-SIFT-IFD method performance is measure, in terms of Recall, Precision, False Measure, Sensitivity, Sensitivity, Accuracy and Gmean.

Keywords: Copy-move forgery detection, Adaptive over segmentation or super pixels Segmentation, Scale-invariant feature transform, Artificial neural network classification.

1. Introduction

Image Forgery (IF) Detection technique is one of the important research areas in the image processing. Digital media are leading technology in the present-day. In Passive approach a digital signature is embedded into the original image. The performance of digital signature is evaluated by checking the condition of the received image. IF Detection techniques are classified into two categories, such as active and passive (blind). The Robust Secret Key (RSK) method is used to protect the images against forgery [1]. Copy move (CM) forgery is the famous and common method to copy and paste elsewhere in the same image. The image processing tools such as Adobe Photoshop, GIMP is used by forgeries for changing the contents of digital images (DI). The forging of an image is not a new issue. Digital signature and Digital watermarking are used for authenticating the content of the DI's [2]. A hybrid method for CM IF is used to identify the changes in the original image.

To alter the information, picture processing tools are used for changing the unique data like blurring and resizing the images. Picture tampering is categorized into non-copy and copy alterations [3]. Manipulation operation is used for deleting hiding images. The detection of Image forgeries is important and active techniques in the research field. Active FD methods are used in the digital watermarking and digital signature technique [4]. Image hashing, Semi-fragile Watermarking and Passive techniques are the most challenging techniques in the image forgeries. Convolution NN (CNN) techniques are used in the new IF detection [5]. DI and video have high importance in our daily life.

The image editing software like Adobe Photoshop and DI are used to do the image forgeries. Active methods are classified mainly into digital signature and watermarking methods. The passive

techniques do not need any explicit prior information of the image. Digital techniques are divided into five main categories such as the format based, pixel-based, physic-based, camera-based and geometry-based methods. Discrete Cosine Transform (DCT) method is used for detecting the forgery in the original images [6]. Nowadays, World Wide Web (WWW) contains a lot of DI for the effective communication process. Most preferred operations in image tampering are i) hiding or deleting a region in the image ii) adding a new object into the image iii) Misrepresenting the image information. CM image tampering is one of the frequently used techniques to manipulate or hide the content of the image. CM FD consists of feature extraction, copy decision and matching methods [7]. The CM and splicing are the most common types of digital IF in image processing techniques. CM forgery is a manipulation technique used to achieve when copying a region of an image and pasting the same image in different locations. The edge information is used in localize forged area when it is not double compressed [8].

The IF is a common malpractice. In DI forgeries, the pixel is the basic building elements of the DI. Nowadays, the digital cameras have single CMOS sensor and use Color Filters Array (CFA) [9]. Nowadays, low-cost digital cameras and cell phones are commonly used in all places. Generally used in many fields such as journalism, medical imaging and forensic investigations. The detecting CM forgery images are used to overlap square blocks. DCT is used to extract feature vectors from the blocks [10].

Based on the existing analysis, to Improve the IF detection accuracy, and minimize the time consumption in this paper, new IF detection SPS-SIFT-IFD technique is introduced. In this system is mainly concerned in segmentation, Feature extraction and classification. To improve the segmentation accuracy Adaptive over segmentation (AOS) technique is used, to improve the classification accuracy. SIFT features and DCT features are used. ANN technique is used for classification purpose. The SPS-SIFT-IFD technique improving various performances parameters like Recall, Precision, False Measure, Sensitivity, Sensitivity, Accuracy and Gmean.

This paper is composed as follows. In Section 2, explained related works. Section 3, described the SPS-SIFT-IFD method. Section 4 described the classification. In Section 5, mentioned experimental setup and results and discussion. The conclusion is made in Section 6.

2. Related work

J. Li, X. Li, B. Yang, and X. Sun [11] introduced "Image segmentation based on CM forgery Detection". The matching process consists of two types of methods i) the suspicious pairs of patches with transforming matrix techniques. ii) The em-based algorithm is designed to refine the estimated matrix. These two methods enhance the performance compared to existing methods on a public database. The improvement of detecting speed by means of parallel programming is difficult.

X. Shen, Z. Shi, and H. Chen [12] introduced "Splicing Image FD with Textural Features on the Gary Level Co-occurrence Matrices (TF-GLCM). The TF-GLCM is calculated based on the Difference Block DCT (DB-DCT) arrays to capture the textural information and the spatial relationship between image pixels. TF-GLCM achieved high detection accuracy of 97.54% and 97.73% on CASIA v1.0 and CASIA v2.0. The main drawbacks of the GLCM methods is that it cannot used to DI blind detection and detection of tampered region in the original image.

Tarun Gulati Mehak [13] introduced "Detection of Digital Forgery Image". The block-based and key-point based techniques were used in the CM forgery technique. JPEG compression with noise and blurring was used in detecting the forgery made in the images. The main drawbacks of this method is that it provides less accuracy.

S. Mushtaq, and A.H. Mir [14] introduced "DI Forgery and Passive Image Authentication". The DI forgeries and Passive Authentication techniques were used to discover the forgery regions in the original images. The main advantage of the method is better accuracy but it provides poor robustness of original image clarity.

A. Namdeol, and A. Vishwakarma [15] introduced "CM Image FD using Wavelet Transform". The pixel-based techniques were used to identify the IF in the actual image. The detection of IF is a significant role in finding the original images. The tampering of the image such as a copy-move, resampling, and splicing were used to resize, stretch, addition, rotate and remove any object from the image.

This all related works contains several problems like accuracy, time consuming, Image clarity, and provides poor robustness. To overcome these problems, SPS-SIFT-IFD method is introduced, which improves the detection accuracy (by using DCT and SIFT), time consumption in results.

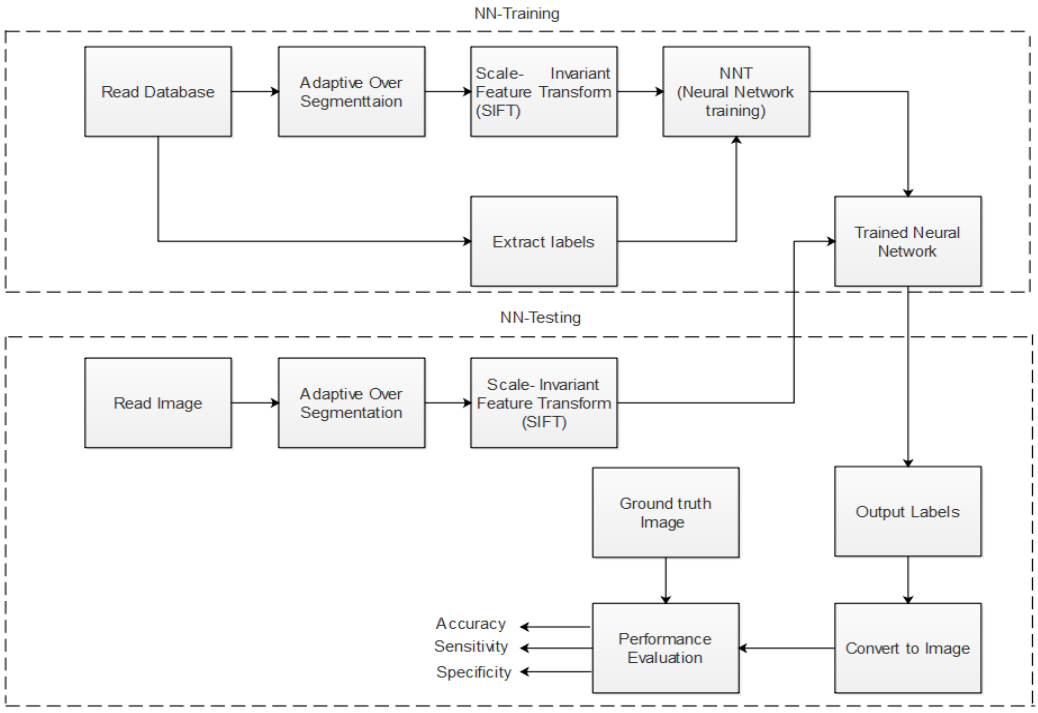

Figure.1 Block diagram of SPS-SIFT-IFD methodology

Figure.2 CM forgery images

3. SPS-SIFT-IFD method

The SPS-SIFT-IFD system is mainly concerned with IF Detection, which is shown in Fig. 1. It consists of three sections which are training, testing and classification. In the testing section the CM pasted images are considered as a forgery image which is taken as an input image for pre-processing. The pre-processed image is given to the AOS or Super Pixels Segmentation (SPS) section, in that the image is divided into the sub-blocks.

For example, some of the CM forgery images are shown in Fig. 2. The next step of the SPS-SIFT-IFD is feature extraction which, consist of three stages such as local color feature extraction, SHIFT FE and DCT feature extraction. This feature extraction is applied for the RGB plains separately. The three features are stored in a single array and which is given to the ANN classifier section. In the training section the feature blocks are trained to ANN and it give to the ANN classifier section. From

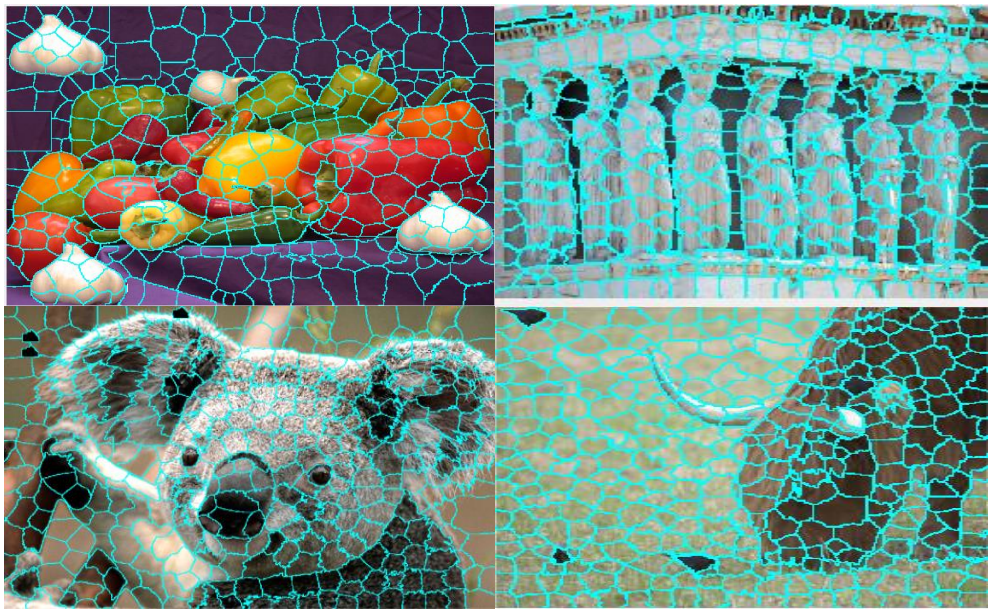

Figure.3 Adaptive over segmentation

the training and testing inputs the ANN classifier classifies the CM forgery part of an image.

3.1 AOS or SPS

The AOS algorithm is similar to host images, which matching computation of the overlapping blocks. To address the existing system problems in SPS-SIFT-IFD the AOS method is introduced. AOS technique segments the host image into a non-overlapping regions (depends upon the shape and the structure host image are separated as a small block). By using matching and classification techniques, this small blocks are classified, from that the forgery region can be detected. In segmentation method, the non-overlapping segmentation decrease the computational expenses compared to overlapping blocking. However, the initial size of the super pixels in SLIC is difficult to decide. In practical applications of CM forgery detection, the host images and the CM regions are of different sizes and have different content, and in our FD method, different initial sizes of the super pixels can produce the different FD results; consequently, different host images should be blocked into the super pixels of different initial sizes, which is highly related to the FD results. For example, AOS is shown in Fig. 3.

3.2 Feature extraction

A digital image consists of many features for example interesting points on the object, which can be extracted to provide a further description of the image. This description can then be used when attempting to locate the object in an image containing many other objects. In our SPS-SIFT-IFD FE five kinds of features is extracted which are SIFT, Standard Deviation (STD), mean, variance and DCT.

3.2.1. SIFT

The SIFT transform provides the images of an object that are unaffected by the object scaling and rotation. SIFT algorithm consist of 4 stage filtering approaches, that are Scale-Space Extrema Detection (SSED), Key point (KP) Key Localistaion (KL), Orientation Assignment (OA) and KP Descriptor.

3.2.2. Scale-space extrema detection

In this stage, the filter identifies the Space location and scale, which is detected from the different views of the object. This can be efficiently achieved using a scale space function that based on the Gaussian function (GF). It is mathematically expressed by Eq. (1):

$$L(x, y, \sigma) = G(x, y, \sigma) \,.\, I(x, y) \tag{1}$$

Where $G(x, y, \sigma)$ is a variable-scale Gaussian, $I(x, y)$ is the input image and . is the convolution operator.

Difference of Gaussians is one such method to detect the KP locations, locating scale-space extrema, $D(x, y, \sigma)$ by computing the difference between two images, one with scale k times the other. $D(x, y, \sigma)$Is expressed as Eq. (2):

$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma) \tag{2}$$

To detect the local maxima and minima of $D(x, y, \sigma)$is compared with the 8 neighbours at the same scale.

3.2.2.1. Key point localistaion

In this stage, to eliminate the more key points and to find the edge, the Laplacian is calculated for each key point in stage 1. The location of extremum, Z, is expressed by Eq. (3):

$$z = \frac{\partial^2 D^{-1}}{\partial x} \frac{\partial D}{\partial x} \tag{3}$$

3.2.2.2. Orientation assignment

This OA targets to assign a consistent orientation to the KP's established based on local image properties. The KP descriptor consider below in Eq. (5). KP descriptor denotes the relative of orientation.

This approach is taken to find an orientation by using the KP to select the Gaussian smoothed image L, from the Compute gradient magnitude m has been calculated by the Eq. (4).

$$m(x, y) = \sqrt{(Lix + 1, y) - L(x - 1, y))^2} + \left(L(x, y + 1) - L(x, y - 1)\right)^2 \tag{4}$$

In the Eq. (5) Compute orientation is consider as 0,

$$A(x, y) = un \frac{(L(x,y+1) - L(x,y-1))}{(Lx+1,y) - L(x-1,y)} \tag{5}$$

Form the gradient orientations of model points which locates the maximum peak in the histogram. This maximum peak creates the key points with orientation.

3.2.2.3. Key point descriptor

The local gradient statistics helps to create KP descriptors. The gradient information is rotated for grouping with the orientation of the KP. Then weighted by a Gaussian variance of 1.5 . KP scale. This data is formerly used to generate a set of histograms over a window centered on the key point. KP descriptors naturally use as a set of 16 histograms, aligned in a 4.4 grid, the 8 orientation bits, one for main compass directions and one of the centre points of these directions. These effects in a feature vector containing 128 origins. The resulting vectors are SIFT key points, which are dependent on the nearest neighbors approach to find the objects in the image.

3.3 Statistical properties

The statistical properties of an image provide a useful information, such as the mean, standard deviation, and variance of the pixel values is expressed in Eqs. (6), (7) and (8).

$$sx = \sqrt{\frac{\sum_{i=1}^{n} (xi - \bar{x})^2}{n-1}} \tag{6}$$

$$mean = 1/n \sum_{N-1}^{n} xi \tag{7}$$

$$varience = \frac{1}{n-1} \sum_{N-1}^{n} (xi - mean)^2 \tag{8}$$

Where,

$$n = number\ of\ data\ points,$$
$$\bar{x} = Mean\ of\ the\ xi,$$
$$xi = value\ of\ data.$$

3.4 Discrete cosine transform (DCT)

$$q(x, y) = cos[\frac{(2x + 1)i\pi}{2N}] cos[\frac{(2y + 1)j\pi}{2N}]$$

$$\mathrm{D(i,j)} = \frac{1}{\sqrt{2\mathrm{n}}} \mathrm{c(i)c(j)} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x, y)\, q(x, y) \tag{9}$$

Where, the x, y element of the image denoted by the matrix p, q is the block that the DCT is done. The equation calculates the one entry of $(i, j)^{th}$ transformed image from the pixel value of the original image matrix.

4. Classification algorithm

Feedforward ANN (FANN) doesn't have any closed paths and the output nodes are linked with the input nodes without any feedback paths. The global minimum is reached by using the Levenberg-Marquardt (LM) algorithm in Back Propagation Algorithm (BPA) and this LM algorithm is used for training the FANN. This neural network has one or more amount of hidden layers of sigmoid neurons followed by an output layer of linear neurons as well as it is used as a general function approximator. The hidden layer has adequate amount of neurons for approximate any function with a finite amount of discontinuities.

The input *j* is given to the FANN in the layer of $l + 1$, which is expressed as follows Eq. (10):

$$m^{l+1-}(j) = \sum_{k-1}^{S_i} w^{l+1}(j, k) b^l(k) + c^{l+1}(j) \tag{10}$$

The output of the FANN is expressed in Eq. (11)

$$b^{l+1}(j) = f^{l+1}\left(m^{l+1}(j)\right) \tag{11}$$

The matrix form of system equations for a N layer network is denoted as and b^0it is expressed as follows Eqs. (12) and (13),

$$b^0 = q \tag{12}$$

$$b^{l+1} = f^{l+1}\left(w^{l+1}b^l + c^{l+1}\right), l - 0.1., \ldots . N - 1 \tag{13}$$

Eqs. (7) and (8) are used to forward the input to the FANN. It absorbs associations among the defined set of input and output pairs such as $\{(q_1, u_1), (q_2, u_2), \ldots (q_R, u_R)\}$.

An approximate decent rule is employed in a back propagation algorithm. The approximate form of the performance index is V and it is expressed as follows Eq. (14):

$$\hat{V} = \frac{1}{2} e_r^U e_r \tag{14}$$

Where, r is the error of the r input and is specified as $e_r = u_r - b_r^N$ and the squared errors for a single input/output pair is exchanging the total sum of errors.

The approximate steepest (gradient) algorithm is specified as Eqs. (15) and (16),

$$\Delta w^l(j,k) = -\beta \frac{\partial \hat{V}}{\partial w^l(j,k)} \tag{15}$$

$$\Delta c^l(j) = -\beta \frac{\partial \hat{V}}{\partial c^l(j)} \tag{16}$$

Where the learning rate is denoted as β.

The performance index sensitivity is to change the input j at the layer of l and it is expressed as follows Eq. (17):

$$\gamma^l(j) = \frac{\partial \hat{V}}{\partial m^l(j)} \tag{17}$$

By considering Eqs. (5), (9) and (12)

$$\frac{\partial \hat{V}}{\partial w^l(j,k)} = \frac{\partial \hat{V}}{\partial w^l(j)} \frac{\partial w^l(j)}{\partial w^l(j,k)} = \gamma^l(j) b^{l-1}(k) \tag{18}$$

$$\frac{\partial \hat{V}}{\partial c^l(j)} = \frac{\partial \hat{V}}{\partial w^l(j)} \frac{\partial w^l(j)}{\partial c^l(j)} = \gamma^l(j) \tag{19}$$

The weight and offset updating process is accomplished by using Eqs. (16), (17), (18) and (19). The recurrence relation is satisfied by the sensitivities and it is specified as γ^l

$$\gamma^l = F^l(m^l) w^{l+1} \gamma^{l+1} \tag{20}$$

The initialized final layer recurrence relation as below Eq. (21):

$$\gamma^l = -F^N(m^N)(u_r - b_r) \tag{21}$$

Where Eqs. (15) and (16) propagate the sensitivities back.

The back propagation is a steepest algorithm is executed and the LM algorithm is used to approximate the newton's method. The function $V(y)$ is minimized with respect to the parameter (y). The Newton's method written as follows Eq. (22):

$$\Delta y = [\nabla^2 V(y)]^{-1} \nabla V(y) \tag{22}$$

Where the HM is denoted as $\nabla^2 V(y)$, the gradient is represented as $\nabla V(y)$, y is expressed as Eq. (23),

$$y = [w^1(1,1) w^1(1,2) \ldots w^1(S1, Q) c^1(1) \ldots c^1(S1) w^2(1,1) \ldots . c^N(S, N)]^T \tag{23}$$

If the $V(y)$ is the sum of squares function, then

$$V(y) = \sum_{j-1}^{M} e_j^2(y) \tag{24}$$

Where M is expressed as following Eq. (25),

$$M = R \times SN \tag{25}$$

The HM and gradient is expressed as following Eqs. (26) and (27):

$$\Delta V(y) = J^T(\mathrm{y}) \mathrm{e}(\mathrm{y}) \tag{26}$$

$$\nabla^2 V(y) = J^T(\mathrm{y}) \mathrm{J}(\mathrm{y}) + \mathrm{S}(\mathrm{y}) \tag{27}$$

Where $J(y)$ is defined as the Jacobian matrix. The Jacobian matrix is computed by the simple modification in the back propagation algorithm as well as it is used for avoiding the mapping problem in y of Eq. (27) in the neural network. The $J(y)$ expressed in the form matrix as given below Eqs. (28) and (29):

$$j(y) = \begin{bmatrix} \frac{\partial e_{1(y)}}{\partial y_1} & \frac{\partial e_{1(y)}}{\partial y_2} \cdots \cdots & \frac{\partial e_{1(y)}}{\partial y_m} \\ \frac{\partial e_{2(y)}}{\partial y_1} & \frac{\partial e_{2(y)}}{\partial y_2} \cdots \cdots & \frac{\partial e_{2(y)}}{\partial y_m} \\ & & \vdots \\ \frac{\partial e_{m(y)}}{\partial y_1} & \frac{\partial e_{m(y)}}{\partial y_2} & \frac{\partial e_{m(y)}}{\partial y_m} \end{bmatrix} \quad (28)$$

And

$$S(y) = \sum_{j-1}^{M} e_j(y) \nabla^2 e_j(y) \quad (29)$$

These equations are leads to the Levenberg-Marquardt method expressed as Eq. (30),

$$\Delta y = [J^T(\mathrm{y})\mathrm{J}(\mathrm{y}) + \varphi \mathrm{I}]^{-1} \; J^T(y) e(y) \quad (30)$$

If the $V(y)$ is increased, the parameter φ is multiplied some factor that is α. While the parameter φ is small, the process becomes the LM algorithm.

The terms calculated by the standard propagation is expressed in Eq. (31),

$$\frac{\partial \hat{V}}{\partial w^l(j,k)} = \frac{\partial \sum_{n-1}^{SN} er^2}{\partial w^l(j,k)} \quad (31)$$

The standard propagation algorithm with one modification at the final layer is expressed in (32),

$$\Delta^N = -F^N(m^N) \quad (32)$$

In Eq. (32), the back propagation is done at each column of the matrix that is sensitivity vector to produce the one row of the Jacobian.

5. Experimental results and discussion

SPS-SIFT-IFD has implemented using desktop computing environment with a RAM capacity of 8 Gb memory. SPS-SIFT-IFD data set are created to test the method. This Dataset is formed based on 48 high-resolution uncompressed PNG true color images, and the average size of the images are 430 x 431. The data set image is shown in Fig. 4. In the dataset, the copied regions are from the categories of nature, living, man-made and mixed, and they range from overly smooth to highly textured; the CM forgeries are created by doubling, scaling and rotating semantically important image regions.

The obtained output has 95% of Accuracy and similarly more data applied for different samples and the final output is being shown in Fig. 10. For example, here i5.png is considered as an input and the algorithm has described image is shown in Fig.5. The AOS segmentation is the second step of our SPS-SIFT-IFD algorithm in that 300 super pixel is segmented which is being shown in Fig. 6.

The third part of the SPS-SIFT-IFD algorithm is FE which consist of three stages of extraction such as local color feature extraction, SHIFT FE and DCT feature extraction. This feature extraction is applied for the RGB plains separately. The three features are stored in a single array and which is given to the ANN classifier section. The ANN classifier consist of two inputs which are training data and test data. Testing data is an input data and the training data is an ANN train output. The data set images are trained to the ANN. ANN training consist of 155 iterations. NN training tool is shown in Fig. 7.

Figure.4 Training Image for i5.png

Figure.5 Test input Image i5.png

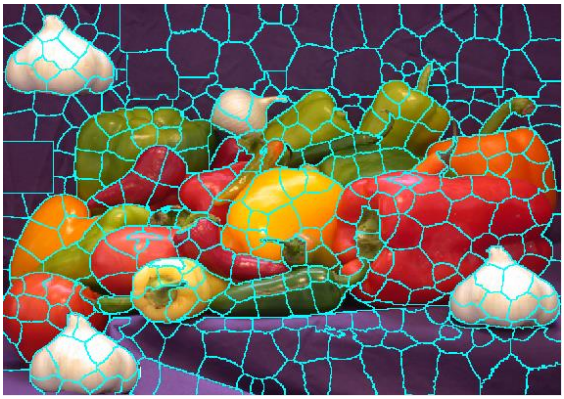

Figure.6 AOS segmented Image i5.png

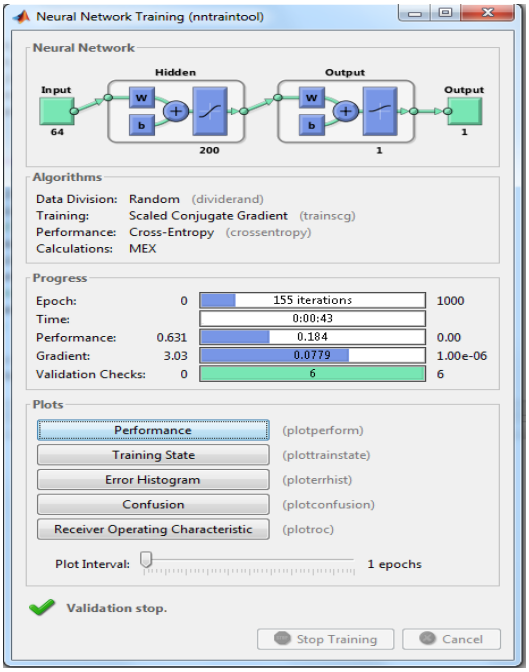

Figure.7 Neural network training tool


Figure.8 Classified forgery, part in i5.png


Figure.9 Segmented forgery, part in i5.png

From the training image ANN classifier classified the forgery parts which is shown in below Fig. 8. After the classification the forgery part is segmented with the help of ground truth image that is shown in Fig. 9. Some other test image outputs are also shown in Fig. 10.

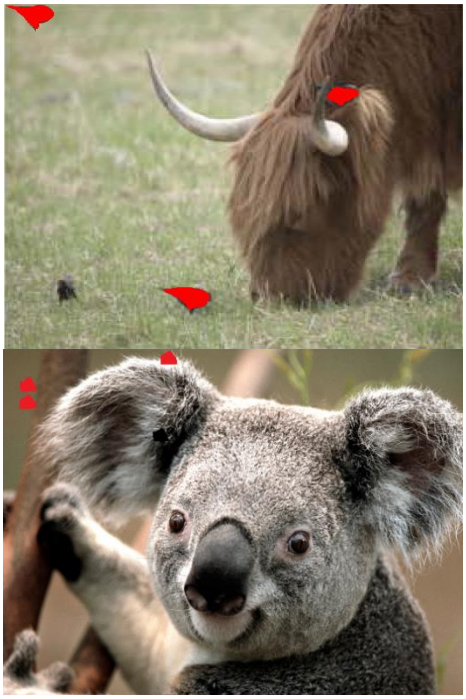
Figure.10 Segmented forgery, part in for other test images

5.1 Recall

Recall is the number of True Positives (tp) divided by the number of (tp) and the number of False Negatives (fn) Recall mathematical equations show as Eq. (33):

$$R = \frac{tp}{tp+fn} \tag{33}$$

5.2 Precision

Precision is the number of tp divided by the number of (tp) and False Positives. It is also called the Positive Predictive (PP) Value. Precision mathematical equations show as Eq. (34):

$$Precision = \frac{tp+tn}{tp+tn+fp+fn} \tag{34}$$

5.3 False measure

A measure that combines precision and recall (r) is the harmonic mean of precision and recall, the traditional F-measure or balanced F-score: False Measure mathematical equations show as Eq. (35):

$$FalseMeasure = \frac{2.R.P}{R+P} \tag{35}$$

5.4 Sensitivity

Sensitivity is a basic property of image

Table 1. Result and comparison

Method	Accuracy	Sensitivity	Specificity	Precision	Recall	F_Measure	Gmean
Existing [16]	0.87941	0.6294	0.9321	0.8256	0.7294	0.6935	0.7941
Existing [17]	0.9345	0.6314	0.9532	0.8352	0.7082	0.7101	0.7952
Existing [18]	0.9456	0.6438	0.9621	0.8125	0.6915	0.7456	0.8035
SPS-SIFT-IFD	0.9531	0.6806	0.9856	0.8487	0.6806	0.7554	0.8190

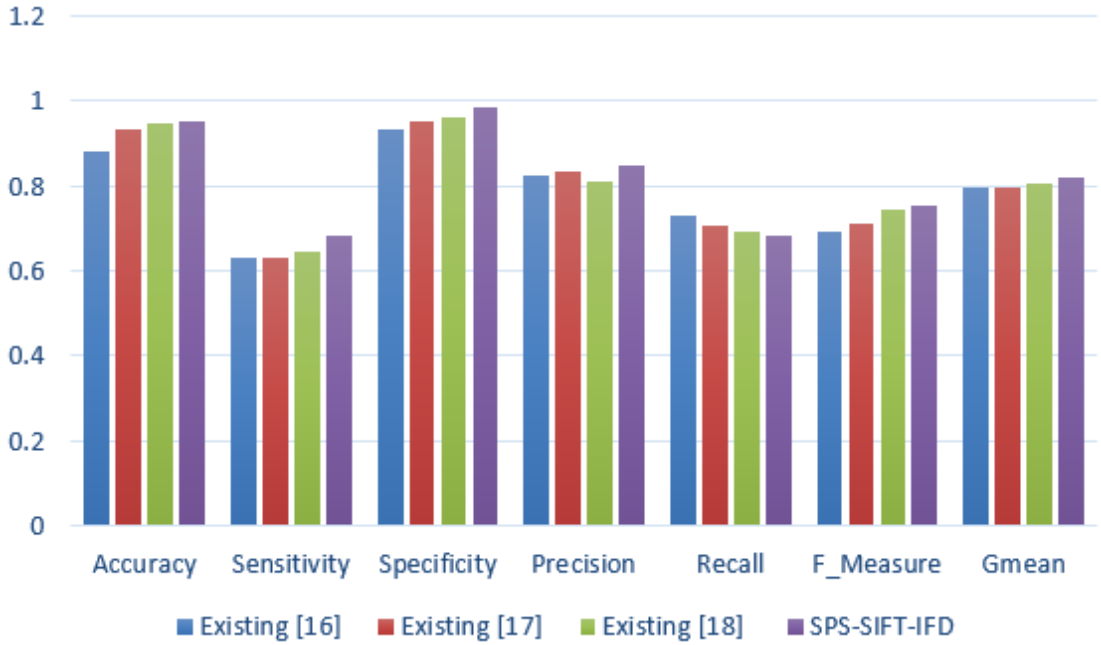

Figure.11 The result and comparison of SPS-SIFT-IFD and existing system [16, 17]

processing the. Sensitivity is also called as tp rate. Mathematically, Sensitivity mathematical equations show as Eq. (36):

$$Sensitivity = \frac{tp}{tp+fn} \tag{36}$$

5.5 Specificity

The specificity provides, how likely the test is to come back negative characteristic. Specificity also called the true negative rate, Mathematically, Specificity mathematical equations show as Eq. (37):

$$Specificity = \frac{tn}{tn+fp} \tag{37}$$

5.6 Accuracy

By using the Specificity and Sensitivity the Accuracy of the image is calculated. Accurately represent the quantity of the image. Mathematically, mathematical equations show as Eq. (38):

$$\text{Accuracy} = \frac{tp+tn}{tp+fp+tn+fn} \tag{38}$$

5.7 Gmean

The F-measure is the harmonic mean of true positive, true negative, false positive and false negative. The G-measure is also called as geometric mean. Mathematically, Gmean mathematical equations show as Eq. (39):

$$tp_{rate} = \frac{tp}{p}$$
$$tn_{rate} = \frac{tn}{p}$$
$$Gmean = \sqrt{tp_{rate}.tn_{rate}} \tag{39}$$

By using the above formulas, the evaluation metrics are calculated. Table 1 shows the performance evaluation and comparison for SPS-SIFT-IFD Vs existing methods [16 - 18]. In that existing systems are implemented by Matlab and tabulated. The existing system [16 - 18] accuracy are 87%, 93%, and 94% SPS-SIFT-IFD system achieved 95% of accuracy, the existing system sensitivity are 62%, 63% and 64% our SPS-SIFT-IFD system achieved 68%, the existing system specificity is 93%, 95% and 96% SPS-SIFT-IFD obtained 98% of specificity. Precision of SPS-SIFT-

IFD system 84% recall decreases up to 3% compared to existing [16], F_measure increase up to the 6% compared to existing [16] and Gmean also increase 2% compared to the existing system [16].

Fig. 11 shows the comparison graph for SPS-SIFT-IFD and existing system [16, 17]. In that the accuracy, sensitivity, specificity, precision, F_Measure and Gmean value are increased, recall, value is decreased.

6. Conclusion

In the SPS-SIFT-IFD method was carried out successfully by using Matlab 2017a with local data set. In this AOS is used for segmentation, SIFT and DCT are used for Feature extraction, and the NN is used for classification. The SPS-SIFT-IFD system is mainly concerned with the feature extraction, three kind of features are taken to improve the performance such as, SIFT, DCT and local RGB colors, the performance measures of SPS-SIFT-IFD system is also compared with the existing forgery detection systems. Compared with the existing system our SPS-SIFT-IFD system provide better detection. SPS-SIFT-IFD system archives 95% of accuracy. In the future work, for further improving the classification accuracy, hybrid optimization techniques and hybrid classification techniques can use.

References

[1] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copy–move forgery detection", *IEEE Transactions on Information Forensics and Security*, Vol.10, No.11, pp.2284-2297, 2015.

[2] A. Khan, S. Ambreen Malik, A. Ali, R. Chamlawi, M. Hussain, M. Tariq Mahmood, and I. Usman, "Intelligent reversible watermarking and authentication: Hiding depth map information for 3D cameras", *Information Sciences*, Vol.216, pp.155-175, 2012.

[3] B. Mahdian, and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants", *Forensic science international*, Vol.171, No.2, pp.180-189, 2007.

[4] Y. Rao, and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images", In: *Proc. of International Workshop on Information Forensics and Security*, pp.1-6, 2016.

[5] H. Moradi-Gharghani, and M. Nasri, "A new block-based copy-move forgery detection method in digital images", In: *Proc. of International Conf. On Communication and Signal Processing*, pp.1208-1212, 2016.

[6] X. Pan, and S. Lyu, "Region duplication detection using image feature matching", *IEEE Transactions on Information Forensics and Security*, Vol.5, No.4, pp.857-867, 2010.

[7] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme", *IEEE Transactions on Information Forensics and Security*, Vol.10, No.3, pp.507-518, 2015.

[8] S. Sadeghi, H.A. Jalab, K. Wong, D. Uliyan, and S. Dadkhah, "Keypoint based authentication and localization of copy-move forgery in digital image", *Malaysian Journal of Computer Science*, Vol.30, No.2, pp.117-133, 2017.

[9] N. Nirmalkar, S. Kamble, and S. Kakde, "A review of image forgery techniques and their detection", In: *Proc. of International Conf. On Innovations in Information, Embedded and Communication Systems*, pp.1-5, 2015.

[10] B. Ustubıoglu, V. Nabıyev, G. Ulutas, and M. Ulutas, "Image forgery detection using colour moments", In: *Proc. of International Conf. On 38th Telecommunications and Signal Processing*, pp.540-544, 2015.

[11] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme", *IEEE Transactions on Information Forensics and Security*, Vol.10, No.3, pp.507-518, 2015.

[12] X. Shen, Z. Shi, and H. Chen, "Splicing image forgery detection using textural features based on the grey level co-occurrence matrices", *IET Image Processing*, Vol.11, No.1, pp.44-53, 2016.

[13] T.G. Mehak, "Detection of Digital Forgery Image using Different Techniques", *International Journal of Engineering Trends and Technology*, Vol.46, No.8, pp.457-461, 2017.

[14] S. Mushtaq, and A.H. Mir, "Digital image forgeries and passive image authentication techniques: A survey", *International Journal of Advanced Science and Technology*, Vol.73, pp.15-32, 2014.

[15] A. Namdeol, and A. Vishwakarma, "A Survey on Copy, Move Image Forgery Detection Using Wavelet Transform", *International Journal of Science and Research*, Vol.4, No.3, pp.876-878, 2013.

[16] Y. Ke, F. Qin, W. Min, and G. Zhang, "Exposing image forgery by detecting consistency of shadow", *The Scientific World Journal*, 2014.

[17] A.S. Alfraih, J.A. Briffa, and S. Wesemeyer, "Forgery Localization Based on Image Chroma Feature Extraction", In: *Proc. of 5th International Conf. on Imaging for Crime Detection and Prevention*, pp.2-11, 2013.
[18] S. Gupta, N. Mohan, and P.S. Sandhu, "Exploiting Noise and Textural Features for Passive Image Forensics", *International Journal of Advanced Research in Computer Science*, Vol.8, No.8, pp.51-53, 2017.