SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

August 2017, Vol. 60 082101:1–082101:18
doi: 10.1007/s11432-016-0478-y

Consistency features and fuzzy-based segmentation for shadow and reflection detection in digital image forgery

Rajan CRISTIN[1]* & Velankanni CYRIL RAJ[2]

[1] *St. Peter's Institute of Higher Education and Research, Chennai, India;*
[2] *Dr. M.G.R Educational and Research Institute University, Chennai, India*

Received July 12, 2016; accepted September 8, 2016; published online April 24, 2017

Abstract Advances in photo editing software have made it possible to generate visually convincing photographic forgeries which have been increased tremendously in recent years. In order to alleviate the problem of image forgery, a handful of techniques have been presented in the literature to detect forgery either in shadow or reflection. This paper aims to develop a technique to detect the image forgery either in shadow or reflection using features enabled neural network. The proposed technique of image forgery detection contains three important steps, like segmentation, feature extraction and detection. In segmentation, shadow points and reflection points are identified using map-based segmentation and FCM clustering. Then, feature points from the shadow points and reflective parts are extracted by considering texture consistency and strength consistency using LVP operator. The final step of forgery detection is performed using the feed forward neural network, where a new algorithm called ABCLM is developed for training of neural network weights. The performance is analyzed with four existing algorithms using measures such as accuracy and MSE. From the analysis, we understand that the proposed technique obtained the maximum accuracy of 80.49%.

Keywords image forensics, forgery detection, shadow, reflection, texture, neural network

Citation Cristin R, Cyril Raj V. Consistency features and fuzzy-based segmentation for shadow and reflection detection in digital image forgery. Sci China Inf Sci, 2017, 60(8): 082101, doi: 10.1007/s11432-016-0478-y

1 Introduction

Digital imaging is a leading technology to create, process and store pictures. Instead of its several advantages, it can be easily misused for doing forgery because the digital images are handled in a way that the forgery cannot be visually detected. Actually, there is a serious attention towards the security problem of the digital content and several techniques [1, 2] have been formulated to authenticate the truthfulness of digital images. Recently, the technical community is paying attention towards the digital image forgery detection area [3]. In literature, two kinds of image forgery such as shadow effect and reflection effects are discussed. While tampering with photos, shadows are the essential parts of an image and some properties in shadows can be used to detect image forgeries [4–6]. The reflection effects for the photos can be synthetically generated by image editing software.

* Corresponding author (email: rcristin2015@gmail.com)

© Science China Press and Springer-Verlag Berlin Heidelberg 2017

The light source and the occluding object together form the shadow and it is prompt in the detection of forgery images. The arrangement of shadows is similar even if they alter in its geometric appearance because of the distinct shapes of the occluding objects and the receiving plane. The shadow is formed when the occluding object obstruct the light from the light source to the plane receiving the shadow. The region which receives the shadow is classified into umbra (dark) and penumbra (less dark) areas. In the umbra area of shadow, the light source is totally hidden by occluding object. In the penumbra area, the light source is hidden partially. If the light source is not point source or when the occluding object cause diffraction of light, then penumbra appears [7]. When the light from a source bounces off a surface and then penetrate the aperture of plane mirror, reflection occurs. If any object is placed in front of the plane mirror, large number of light rays from the object will fall on the mirror in various directions and the incident light rays are reflected by the mirror. Then the image is generated in a place in which all the reflected light rays intersect and also the ray between the image and the object should appear to be perpendicular to the reflecting plane [8].

To interpret image forgery, particularly to handle shadow and reflection, several tools and methods have been developed by the researchers in past years. The existing digital image forensic techniques are broadly classified as Pixel-based techniques and Geometric-based techniques [9]. The pixel-based technique examines the pixel-level correlation which occurs from specific form of tempering such as splicing, cloning and re-sampling [10–12]. In this technique, the goal of detecting original or forgery image is the classification of given images into two classes namely authentic (original) and forged images. The existing image forgery detection techniques extract the image features and then select a classifier. The features extracted from the image set are used to train the classifier. Finally, the features are classified. The geometric-based techniques make use of the contradiction in the object's reflection [13] to detect the forgery in the image. The detection is based on the contradiction in the reflection or shadow of the image. This method has a drawback that the features must be selected accurately, which is difficult to be satisfied in the case of images that are not clear. Also, if the lines are almost parallel, then its shadow or reflection is tentatively positioned at infinity. In such conditions, small variation in the feature selection may results in large error distance. When comparing with the geometric constraint methods [5, 6, 10], pixel based methods are easy and it performs well in the condition that the shadow is copied and pasted in another location in the same image.

In this paper, consistency-based features and neural network are utilized to design and develop a method for shadow and reflection detection in digital image forgery. The proposed method consists of three major steps: (1) Shadow segmentation. (2) Reflected image segmentation. (3) Shadow and reflection detection. In the first step, the shadow part of images is effectively segmented using the shadow candidate map given in [14]. Similarly, reflected and the original image is segmented using the fuzzy c-means clustering. Then, forgery detection of image is done with the neural network classifier using the necessary information of texture consistency, strength consistency shadow and reflective factors. Texture consistency, strength consistency –based parameters is effectively estimated using local vector pattern [15] which is one of the recent and effective techniques for texture descriptors of images. Finally, shadow and reflective factors are estimated from the segmented results and additionally included to estimate the forgery image.

The main contributions of the paper are given as follows:

- A forgery in shadow or reflection is detected within the single framework using the neural network classifier and Local Vector Pattern (LVP) [15].

- Neural network training process is modified with the proposed learning algorithm, called ABCLM, where Levenberg Marquardt algorithm (LM) [16] and Artificial Bee colony (ABC) algorithm [17] are effectively integrated.

The paper is organized as follows: Section 2 presents motivation behind the approach. Section 3 explains the proposed technique of consistency features and fuzzy-based segmentation for image forgery detection. Section 4 presents the experimentation of the proposed technique and Section 5 summarizes the conclusion of the paper.

Table 1 Literature review

Authors	Contribution	Forgery detection	Issues
Ke et al. [9]	Texture consistency and strength consistency-based technique	Shadow	Stability of the detection is questionable
Kee et al. [4]	Projection and linear programming-based method	Shadow	Computation overhead to solve the LP problem
O'Brien and Farid [13]	Reflective geometry and linear perspective projection-based method	Reflection	Requires multiple points for the projection space
Kee et al. [18]	Geometric technique with projected location	Shadow	Accurately estimating light source is difficult
Yang et al. [7]	Support vector machine with scale factors	Shadow	Detecting shadow lines through SVM require more complex training data
Cao et al. [19]	Sun elevation with geometric constraints	Shadow	Including multiple geometry constraints have the problem of estimating the focal length
Ge and Malik [8]	Normalized error distance and geometry	Reflection	Distance is more dependent on the uncertain features

2 Motivation behind the approach

2.1 Literature review

Literature presents various techniques for image forgery detection using texture and geometric-based technique (Table 1). The geometry-based techniques are discussed in [8, 13, 18, 19] which calculates the geometric properties from the images for digtal forgery estimation. The learning algorithms are also applied to image forgery detection in [4, 7] where, a priori knowledge of image forgery is trained using training algorithm and the detection is performed using the trained processes.

2.2 Problem definition

Due to the ever increasing development of photo editing software, images are tampered from the original scene to hide the original content in the image or hiding the hidden truth from the original content. This hidden information may pose wrong decision for the investigator from forensics department. So, the detection of forgery or tampered images is very important for this digital world. Let us assume that D is a database having different images which may be tampered shadow image, tampered reflected image, original shadow or original reflection images. So, totally U categories of images are in the database. This is represented as $D = \{c_i; 1 \leqslant i \leqslant U\}$. Each category of image contains N different images, $c_i = \{\mathrm{IM}_j; 1 \leqslant j \leqslant N\}$, where the image is represented as IM. The objective here is to detect the forgery images which may be a tampered shadow or a reflected image.

2.3 Challenges

Due to the continuous growth of image communication, attackers try to do forgery through this visual imagery which poses a challenge about the integrity of the imagery. One of the forgeries continuously happening in real life is image manipulation which can be in various ways like resizing, filtering, shadowing and reflection. Here, manipulation through shadowing and reflection makes a significant impact on the integrity of the image. So, detection of fraudulent shadows and the reflection is an important topic to be solved. In shadow and reflection forgery detection, the following major challenges should be addressed

- The detection of forgery shadow seems tough when the objects are in various heights from the ground or different distance from the mirror objects.
- The challenge of identifying the intensity variation for the real shadows and fraudulent shadows become difficult because of advanced photo editing software which considers the real fact that shadows are formed when an opaque object comes in the path of light, to simulate the shadows or reflections.

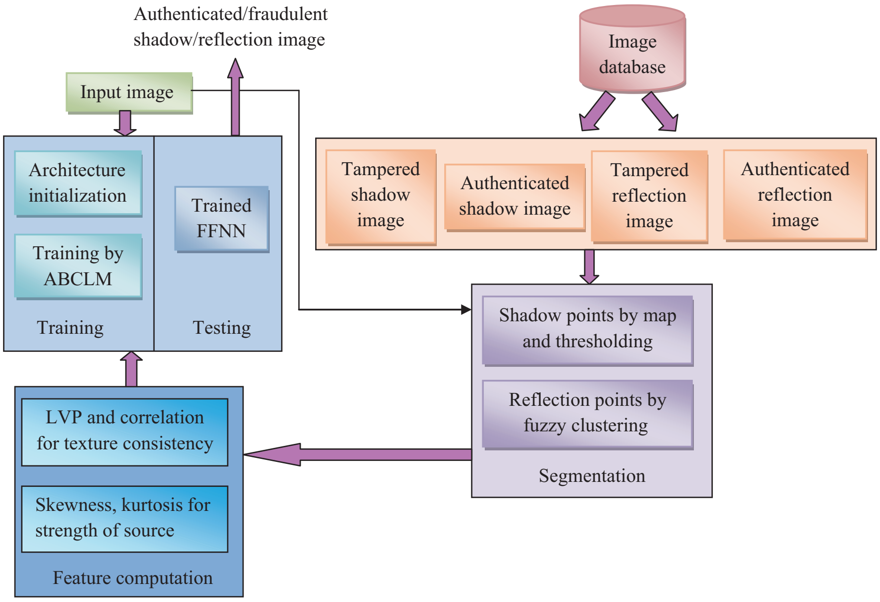

Authenticated/fraudulent shadow/reflection image
Input image
Architecture initialization
Training by ABCLM
Training
Trained FFNN
Testing
Image database
Tampered shadow image
Authenticated shadow image
Tampered reflection image
Authenticated reflection image
Shadow points by map and thresholding
Reflection points by fuzzy clustering
Segmentation
LVP and correlation for texture consistency
Skewness, kurtosis for strength of source
Feature computation

Figure 1 (Color online) Block diagram of the forgery image detection.

- The parallel detection of forgery images due to shadow and reflection face the additional problems of handling the different shape and size of the shadow and reflection in detecting the forgery images.
- Literature presents different techniques for exposing image forgery through image shadows. One of the work presented in the literature [9] considered the detection based on the texture and strength of the source light based on the similarity value where the threshold is given to find the image forgery. The fixing of threshold and its corresponding manipulation is difficult to fix up for every image automatically.
- Also, Local Binary Pattern (LBP) [9] is used for texture descriptor which is one of the traditional methods for texture description.

3 Proposed method

This section presents the proposed method of forgery image detection using consistency features and fuzzy-based segmentation. The proposed method read the input database directly and the segmentation of shadow region and reflected region is performed using candidate shadow map and fuzzy clustering method. Once the shadow and reflection regions are extracted, the important feature like strength and texture-enabled features are extracted to identify the forgery images. The forgery detection is performed using the feed forward neural network which effectively classifies the input image using the proposed learning algorithm. Figure 1 shows the block diagram of the proposed technique of forgery image detection.

The proposed method contains four major steps. (i) Determination of shadow points using map-based segmentation. (ii) Determination of reflection points using FCM clustering. (iii) Computation of feature points using shadow and reflective factors. (iv) Forgery image detection using proposed ABCLM-based neural network.

3.1 Determination of shadow points using map-based segmentation

The first step in the proposed forgery image detection is to determine the shadow points using candidate map-based segmentation given in [14]. This method of segmentation identifies the shadow point by mapping the original image into shadow map image and then thresholding is applied for binary segmentation. This process is performed using two important steps like, computation of shadow map and segmentation of shadow points using Otsu's threshold.

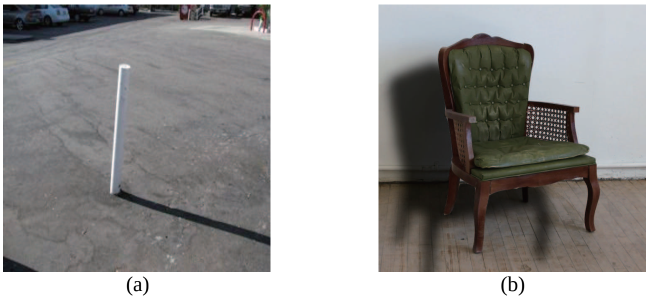


Figure 2 Sample input images. (a) Original shadow image; (b) forgery shadow image.

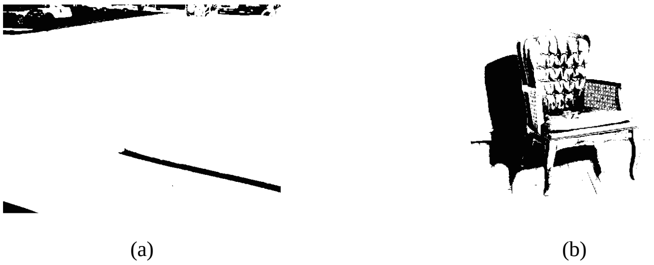


Figure 3 Determination of shadow points. (a) Segmented original shadow image; (b) segmented forgery shadow image.

(a) Computation of shadow map: Let us assume that the input image IM is given to normalization step to convert the image into normalized data. Once the normalization is finished, gamma γ is used to level the input image using the following equation,

$$L = \mathrm{IM}^{\frac{1}{\gamma}}, \quad G = R^{\frac{1}{\gamma}}, \tag{1}$$

where IM is the input image and G is the red band of the image scaled with gamma γ. Then, the exponential function is used to convert the image space into kernel space. Here, the gray scale image L and the red band of the input image G are processed separately with the exponential function.

$$S_c = \frac{1}{1 + \mathrm{e}^{-a[(1-L)-b]}}, \tag{2}$$

$$S_R = \frac{1}{1 + \mathrm{e}^{-a[(1-G)-b]}}, \tag{3}$$

where S_c and S_R are the kernel grayscale image which is obtained based on L and G, a and b are the kernel weight constants. Then, kernel grayscale image and red band image is processed with the following equation to find the candidate shadow map. Here, T is a threshold given by the user.

$$S = (1 - (S_c * S_R)) * (1 - T). \tag{4}$$

Figure 2 shows the sample input images of original and forgery images. Figure 3(a) shows the shadow map extracted from the forgery shadow image.

(b) Segmentation of shadow points using Otsu's threshold: The shadow map is directly given to the binary segmentation algorithm which identifies the shadow points separately. The identification of shadow points from the gray scale shadow map image is performed using the automatic thresholding technique devised in [20]. The automatic threshold is used to convert the gray scale image into binary image where, the shadow points are extracted separately. Figure 3(b) shows the segmented shadow image.

3.2 Determination of reflection points using FCM clustering

The second step is to perform fuzzy c-means clustering on the input image to identify the region belonging to the reflection. Clustering-based segmentation is one of the simple methods to identify the dissimilar

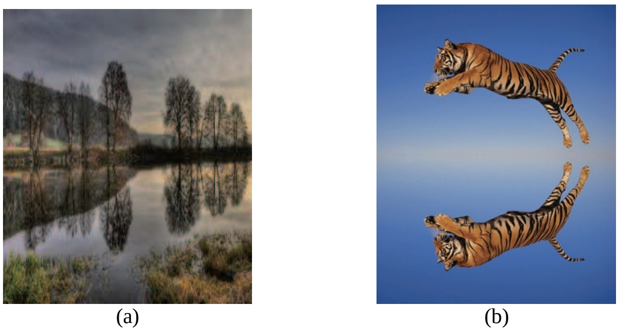


Figure 4 (Color online) Sample input images. (a) Original reflection image; (b) forgery reflection image.

regions from the input image. Here, we have considered the popular clustering algorithm, called FCM [21], which is developed by integrating the fuzzy concept in finding the cluster centroids.

(a) Fuzzy-based segmentation: The fuzzy based segmentation method is employed to resolve the issue of overlapping of data points and also comparatively better than k-means algorithm. In order to perform fuzzy based segmentation on the input image, the image is transformed to data matrix, where the number of data objects is equivalent to the number of pixels in the image and the number of attributes is equivalent to the intensity of the corresponding pixel and its neighbor pixel. Then, FCM clustering is performed on the data matrix to identify the dissimilar regions. Let us assume that P_i is the pixel information and n is the total number of pixels. Then, the process of grouping the similar pixels are given as follows: (i) Initialize the membership matrix randomly in the size of $n \times q$, where q is the number of groups required. (ii) Compute the centroids based on the following equations,

$$m_j = \frac{\sum_{i=1}^{n} e_{ij}^{b} . P_i}{\sum_{i=1}^{n} e_{ij}^{b}}, \tag{5}$$

where e_{ij}^{b} is the fuzzy membership matrix, P_i is the pixel information, and n is the number of pixels. (iii) Update the membership matrix using the centroids m_j and the pixel information P,

$$e_{ij}^{b} = \frac{\|P_i - m_j\|^{\frac{-1}{b-1}}}{\sum_{j=1}^{q} \|P_i - m_j\|^{\frac{-1}{b-1}}}. \tag{6}$$

Steps (ii) and (iii) given above should be executed until there is no difference in the cluster centroid. Once, the centroids are found, the grouping is performed by assigning the most similar pixel into its corresponding centroids so that we can obtain the q number of clusters. Figure 4(a) shows the sample authenticated reflection images and Figure 4(b) shows the forgery reflected images.

(b) Extracting reflective point using candidate similarity measurement: This step is used to identify the reflection regions from the groups identified from the previous steps. Each group centroids are used to find the pair wise similarity and the two groups having most similar are known to be original object and its reflected contents. Then, the cluster lesser in size out of the selected two clusters is taken as the reflected object. Figure 5(a) shows the FCM results of the forgery reflected image and Figure 5(b) shows the extracted reflective region.

3.3 Computation of feature points using shadow and reflective factors

This step is intended to extract the feature points from the shadow point and reflective parts. Here, two different variety of features are extracted based on the texture consistency and strength consistency

(a) Texture consistency feature: To extract the texture consistency feature, Local Vector Patten (LVP) [15] is utilized since the forgery objects do not significantly change texture properties of the background region. Basically, the LVP pattern is the high order derivation function for the texture descriptor. In order to extract the texture consistent feature, the LVP use the four pairwise direction of the vector of the current pixel with the neighbourhood or surrounding pixels. Thus, the LVP pattern rather than the

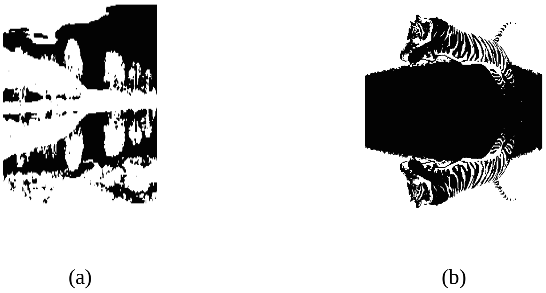


Figure 5 Determination of reflection points. (a) Segmented original reflection image; (b) segmented fraudulent reflection image.

other descriptor is robust against the rotational invariant of the image and also solves the dimensionality reduction issue. Let us assume that I be the input image which is used to compute the direction vector based on the reference pixel r,

$$V_{\beta}^{d}(r) = I(\beta, d) - I(r), \tag{7}$$

where β indicates the direction, r indicates the pixel location and d denotes the distance. The LVP $L_d(r,\beta)$ in β direction of vector at r is mathematically given as

$$L_d(r,\beta) = \sum_{k=1}^{N_p} 2^{k-1} f_d(k,r,\beta), \tag{8}$$

where $L_d(\cdot)$ refers to the LVP at neighborhood distance d and β is the index angle.

$$f_d(k,r,\beta) = \begin{cases} 1, & F_{k,r,\beta}^{d} \geqslant 0, \\ 0, & \text{otherwise}, \end{cases} \tag{9}$$

$$F_{k,r,\beta}^{d} = V_{\beta+45^\circ}^{d}(k) - \left[\frac{V_{\beta+45^\circ}^{d}(r)}{V_{\beta}^{d}(r)} \times V_{\beta}^{d}(k)\right], \tag{10}$$

where N_p is the number of neighbor pixels considered. The finding of $F_{k,r,\beta}^{d}$ is based on the pixels which are located at β angle from the input pixel r.

(b) Strength consistency of light of source: Strength consistency is computed with the assumption that the strength of the light source obtained from shadows should be consistent in all the parts of the image. Usually, the forgery images are created by copying the main body, its shadow, and surrounding regions from another image and pasting it to the original image. Henceforth, strength of light source is varied significantly in the shadow region as well as the original content region. This variation of strength of the light source can be utilized to detect tampering.

(c) Feature extraction: For detecting the tampered images, 18 set of features are utilized. The texture image obtained from the LVP is separated into non-shadow part and shadow part. Subsequently, histogram vector is computed from both the regions separately and the correlation coefficient is computed from these two regions.

$$z_1 = \mathrm{rC}\left(\mathrm{LVP}(I_{\mathrm{sha}}), \mathrm{LVP}(I_{\text{non-sha}})\right), \tag{11}$$

where $\mathrm{LVP}(I_{\mathrm{sha}})$ is the LVP of the shadow image, and $\mathrm{LVP}(I_{\text{non-sha}})$ is the LVP vector of non-shadow image. $\mathrm{rC}(\cdot)$ is the correlation function defined as

$$\mathrm{rC} = \frac{\sum_{i=1}^{N_T}(u_i-\bar{u})(t_i-\bar{t})}{\sqrt{\sum_{i=1}^{N_T}(u_i-\bar{u})^2}\sqrt{\sum_{i=1}^{n}(t_i-\bar{t})^2}}, \tag{12}$$

where $\bar{u}$ is the mean of the LVP of the shadow image, $\bar{t}$ is the mean of the LVP vector of non-shadow image, u_i is the elements of the LVP of the shadow image and t_i is the element of the LVP of the non-shadow image.

Table 2 Sample feature set

	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}	z_{13}	z_{14}	z_{15}	z_{16}	z_{17}	z_{18}
I_1	0.87	0.03	0.59	1.73	0.02	−0.22	1.73	0.14	5.57	0.78	0.02	−0.71	3.2	0.23	1.76	4.15	0.44	6.13
I_2	0.97	0.01	0.37	2.69	0.01	0.32	2.38	0.24	5.13	0.98	0.11	−1.43	3.92	0.03	−0.77	2.81	0.49	6.73
I_3	0.89	0.03	−0.88	2.85	0.02	−0.64	2.61	0.09	5.53	0.95	0.05	1.78	4.2	0.03	0.43	1.43	0.85	6.34
I_4	0.95	0.04	0.44	2.37	0.05	0.15	3.39	0.24	5.79	0.91	0.1	−0.8	3.52	0.04	2.23	11.28	0.7	6.84

Then, to compute the strength of light source, standard deviation (σ), skewness (sk) and kurtosis (ku) are computed from the shadow and non-shadow region.

$$z_2 = \sigma\left(I_{\text{sha}}\right), \tag{13}$$

$$z_3 = \sigma\left(I_{\text{non-sha}}\right), \tag{14}$$

$$z_4 = sk\left(I_{\text{sha}}\right), \tag{15}$$

$$z_5 = sk\left(I_{\text{non-sha}}\right), \tag{16}$$

$$sk = \frac{\frac{1}{N_T}\sum_{i=1}^{N_T}\left(p_i-\bar{p}\right)^3}{\left[\frac{1}{N_T-1}\sum_{i=1}^{N_T}\left(p_i-\bar{p}\right)^2\right]^{3/2}}, \tag{17}$$

$$z_6 = ku\left(I_{\text{sha}}\right), \tag{18}$$

$$z_7 = ku\left(I_{\text{non-sha}}\right), \tag{19}$$

$$ku = \frac{\frac{1}{N_T}\sum_{i=1}^{N_T}\left(p_i-\bar{p}\right)^4}{\left[\frac{1}{N_T}\sum_{i=1}^{N_T}\left(p_i-\bar{p}\right)^2\right]^{2}} - 3, \tag{20}$$

where $\sigma(\cdot)$ is the standard deviation, $\bar{p}$ is the mean of the image, p_i is the pixel elements of the image and N_T is the total number of pixels in the image. Then, the mean of the shadow image $\bar{p}$ and entropy of the shadow image is also utilized.

$$z_8 = \bar{p}, \tag{21}$$

$$z_9 = \sum_{i=1}^{U_s} pr_i * \log(pr_i), \tag{22}$$

where $\bar{p}$ is the mean of the shadow image, pr_i is the probability of the symbols in the shadow image, and U_s is the unique symbols in the shadow image.

For the detection of the tampered reflected images, the same set of features is extracted from the reflected and original objects. So, totally, 18 feature set for every image are extracted to identify the original and forgery images. The final feature representation for the input image I is given as follow.

$$Z = \left\{z_1, z_2, \ldots, z_{18}\right\}. \tag{23}$$

Table 2 tabulates the sample set of features extracted from four different images given in Figures 2 and 4. In Table 2, I_1 is the original shadow image, I_2 is fraudulent shadow image, I_3 is the original reflected image and I_4 is fraudulent reflected image.

3.4 Forgery image detection using proposed ABCLM-based neural network

The final step is to perform forgery image detection using the feed forward neural network (FFNN) [22]. Neural network is much suitable to perform multi-classification as compared with other classifiers like SVM, fuzzy classifier, k-NN classifier and naïve Bayes classifier. Traditional SVM is a binary classifier which is well suitable to perform two level classifications. Even though it is adapted to perform multi level classification using ‘one versus all’, the performance is not much convincing. This is the reason to select neural network for the four level of classification.

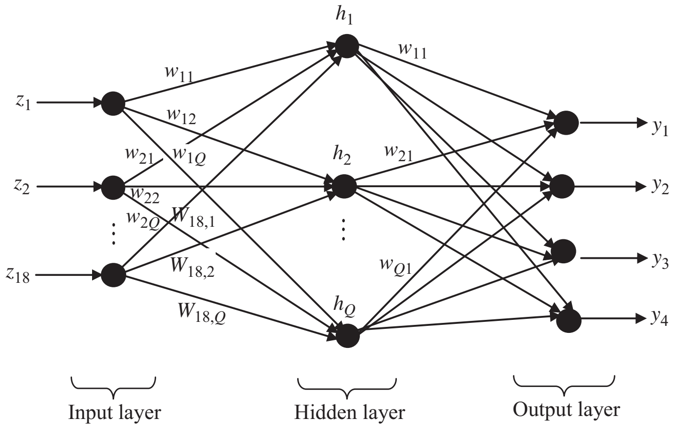


Figure 6 Architecture of feed forward neural network.

The classification we performed here is the image level classification. The aim is to find whether the image is related to original shadow, original reflection, fraudulent shadow or fraudulent reflection based on the segment feature. Here, the features extracted from the images are given for learning purpose. Once the neural network effectively learns the weights, it can easily detect whether the image is forgery or authenticated using the features.

(a) Initialization of FFNN architecture: Initially, the architecture of FFNN should be properly designed for identification of weights which are fit for performing the classification. Here, our aim is to do the classification using 18 different features so the input layer contains 18 neurons. The detection of four different categories is to be performed using neural networks. So, the output layer contains four neurons. The hidden neurons and hidden layers can be fixed optimally for better classification. Figure 6 shows the architecture of FFNN utilized in this work.

(b) Neural network training by the proposed ABCLM algorithm: Neural network training is the process of identification of the weights that is fit for the neural network which can classify the input image. The finding of optimal weights is performed using the proposed hybrid learning algorithm which combines the Levenberg-Marquardt algorithm [16] and Artificial Bee Colony (ABC) algorithm [17]. Let the input weights can be represented as

$$W = \left\{w_{ij}^{X};\ 0 \leqslant X \leqslant N_H; 0 \leqslant i \leqslant N_N; 0 \leqslant j \leqslant N_N\right\}, \tag{24}$$

where N_H is the number of hidden layer and N_N is the number of hidden neurons. At first, input weight are initialized randomly. Then, weights are found out using the formula given in the LM algorithm [16] as

$$W_{I+1}^{\mathrm{LM}} = W_I - [H + \mu * \mathrm{ID}]^{-1} * g, \tag{25}$$

$$H = J^{\mathrm{T}} * J, \tag{26}$$

where μ is the Levenberg's damping factor which ranges from 0 to 1. ID is the identity matrix. J is the Jacobian matrix for the system which is obtained by taking the first-order partial derivatives of a vector-valued function. The gradient matrix of g is computed using the following equation,

$$g = J^{\mathrm{T}} * \mathrm{MSE}, \tag{27}$$

where MSE is the mean square error which is obtained by computing error between the original class and the output. The output is obtained by inputting the training data into the neural network. Then, weights are computed using the ABC algorithm [17]. The formula used for finding the weight matrix is given as follows:

$$W_{I+1}^{\mathrm{ABC}} = W_I + \Phi * \left(W_I - W_{I+1}^{\mathrm{LM}}\right), \tag{28}$$

where Φ is an adjusting factor slowing down the convergence speed as the evolution goes. Once two new weights are computed from the LM and ABC algorithm, two errors such as $\mathrm{MSE}^{\mathrm{LM}}$ and $\mathrm{MSE}^{\mathrm{ABC}}$ are

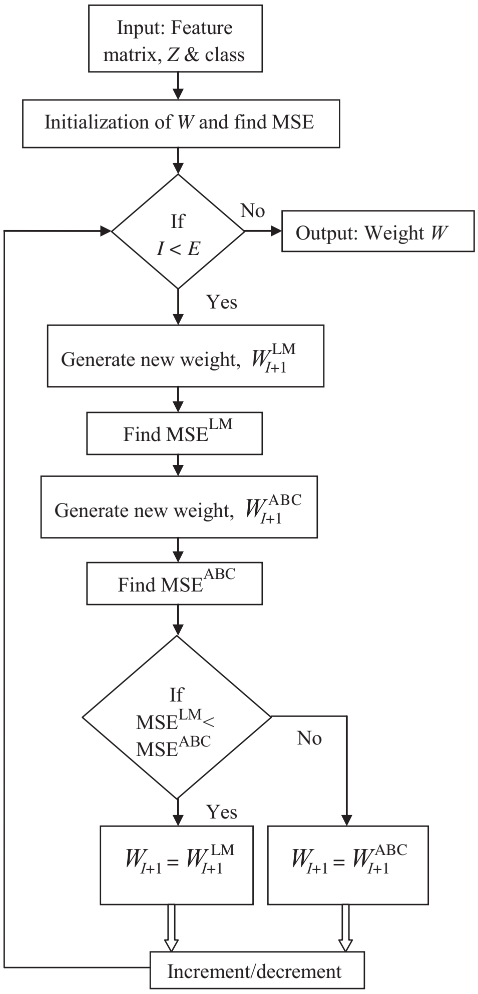

Input: Feature matrix, Z & class
Initialization of W and find MSE
If I < E
No
Output: Weight W
Yes
Generate new weight, W_{I+1}^{LM}
Find MSE^{LM}
Generate new weight, W_{I+1}^{ABC}
Find MSE^{ABC}
If MSE^{LM}< MSE^{ABC}
No
Yes
$W_{I+1} = W_{I+1}^{LM}$
$W_{I+1} = W_{I+1}^{ABC}$
Increment/decrement

Figure 7 Flow chart of proposed ABCLM algorithm.

computed by applying the training data to the neural network function. From the mean square error, the one which is having the less value is assigned as the error value of the current iteration (MSE$_{I+1}$) and its corresponding weight is assigned as the final weights for the current iteration (W_{I+1}). Then, the value of μ is decreased by a factor v if the error value is decreased. Or else, the value of μ is increased by a factor v. This process is repeated for E number of iteration and the final weights are taken as the trained weights which are then used for the detection of fraudulent images. Figure 7 shows the flow chart of proposed ABCLM algorithm.

(c) Forgery detection by trained neural network: For a test image, the features are extracted after performing shadow and reflection segmentation. The extracted features are directly given to the trained neural network which shows whether the input image is fraudulent shadow/reflected image or authenticated shadow/reflected image.

4 Results and discussion

This section presents the experimental results of the proposed image forgery detection and a detailed discussion of the results.

4.1 Experimental set up

The proposed image forgery detection is implemented using MATLAB (R2014a). The system has i5 processor of 2.2 GHz CPU clock speed with 4 GB RAM and 64-bit operating system running with

Windows 8.1. The proposed technique is analyzed with various values of numbers of clusters q, gamma γ, hidden neurons N_N and hidden layer N_H to find the best values for the comparative analysis. Once the parameters are found out from the experiment optimally, the proposed technique is compared with existing work given in [9]. In [9], two methods have been presented, in their first method, texture consistency is taken for the detection and strength of light is taken for detection in the second method.

(i) Dataset description. The experimentation is performed with the dataset collected from the public resources. Here, four categories of images, original shadow or reflected images, and original reflection or fraudulent reflected images, are used. The original shadow and reflected images are collected from the internet, and then shadow and reflection are synthetically created within the images using photo editing software. The authenticity of the collected images is verified by the imaging experts. Here, the total number of images considered is 120 with the resolution of 255 × 255. As the work aims to perform the four level of classification, we have collected 30 images from each category.

(ii) Evaluation metrics. The performance of the proposed forgery detection is evaluated using two parameters, such as accuracy and Mean Square Error. The formula used for computing accuracy, True Positive Rate (TPR) and False Positive Rate (FPR) is given as follows:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FN} + \text{FP}}, \quad \text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \quad \text{FPR} = \frac{\text{FP}}{\text{TN} + \text{FP}}, \tag{29}$$

where True Positive (TP) is correctly identified, False Positive (FP) is incorrectly identified, True Negative (TN) is correctly rejected and False Negative (FN) is incorrectly rejected. The MSE is computed using the following equation,

$$\text{MSE} = \frac{1}{N_T} \sum_{i=1}^{N_T} \left| G_c^i - O_c^i \right|, \tag{30}$$

where N_T is the total number of testing images, G_c^i is the original ground truth class information, O_c^i is the output obtained from the proposed work.

(iii) Methods taker for comparison.

Texture consistency of shadow: The texture consistency [9] between the shadow and image is used for the forgery detection.

Strength consistency of light source of image: The strength variation of the light source [9] is used to detect the forgery images. Here, also, the light source from the shadow and non-shadow region is estimated. Then, the similarity measure is evaluated by the correlation function which detects whether the input image as original or forged image.

LM: The Levenberg-Marquardt algorithm [16] is a second order approach to train the data without Hessian matrix. The LM algorithm improves the efficiency of the system and also provides the good convergence property. In such cases, the efficiency of this method is decreased while increasing the number of weights and then the large amount of memory is also required.

(iv) Visual image results. Figure 8 depicts the experimental results of the fuzzy based segmentation for digital image forgery. In Figure 8(a), the original shadow image is given as the input image. Then, the shadow regions of the input image are detected using the fuzzy c-means based segmentation. Thus, the detection of shadow point is shown in Figure 8(b). Similarly, Figure 8(c) represents the original shadow image after applying noisy information. Thus, Figure 8(d) shows the segmented original shadow images with noisy data.

Subsequently, Figure 9 represents the visual image result using the FCM based segmentation. The Figure 9 (a) and (b) shows the original and segmented shadow image. Similarly, the noisy shadow image is given in Figure 9(c) and its corresponding segmented image using fuzzy based segmentation is in Figure 9(d).

4.2 Performance evaluation of the proposed training algorithm

This subsection presents the performance evaluation of the proposed fraudulent detection technique to find the optimal parameters for numbers of clusters q, gamma γ, hidden neurons N_N and hidden layer

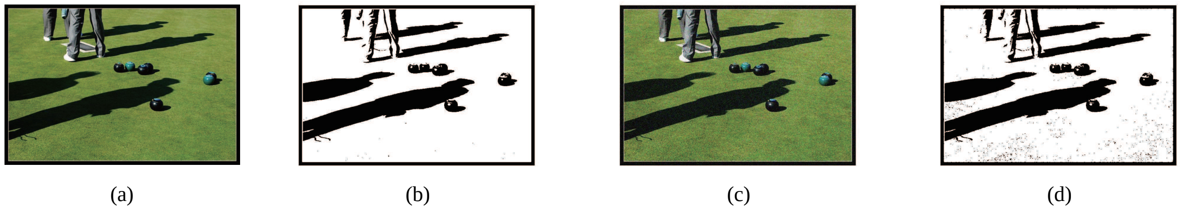

(a) (b) (c) (d)

Figure 8 (Color online) Visual image results for original shadow image 1 and segmented image. (a) Original shadow image; (b) segmented shadow image; (c) noisy shadow image; (d) segmented noisy shadow image.

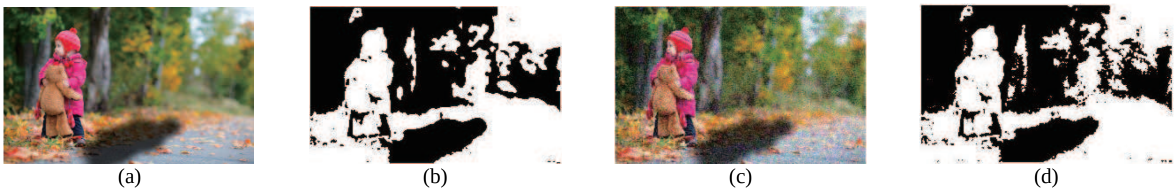

(a) (b) (c) (d)

Figure 9 (Color online) Visual image results for original shadow image 2 and segmented image. (a) Original shadow image; (b) segmented shadow image; (c) noisy shadow image; (d) segmented noisy shadow image.

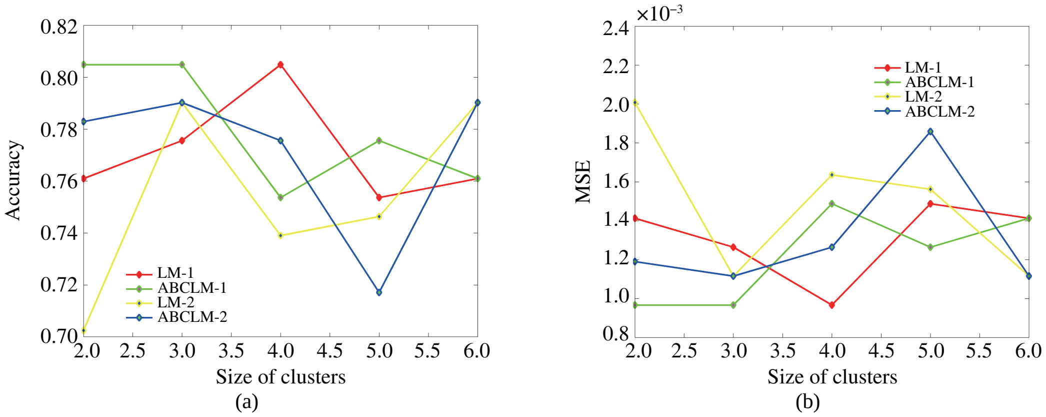
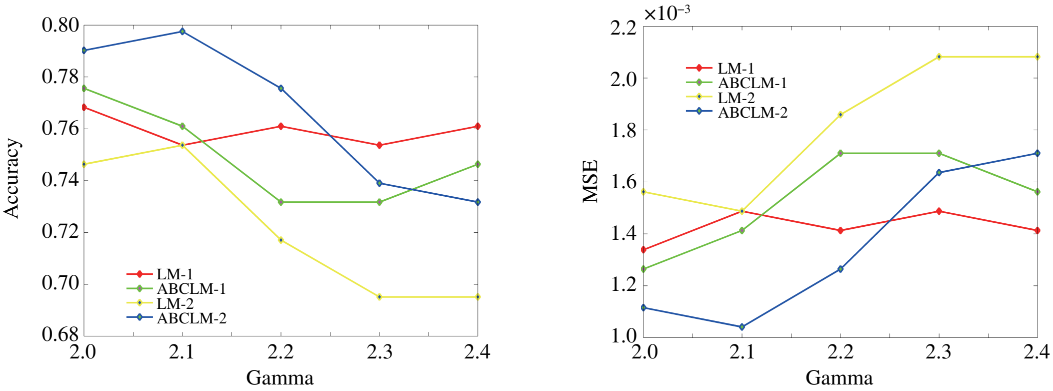


Figure 10 (Color online) Various numbers of clusters. (a) Accuracy; (b) MSE.

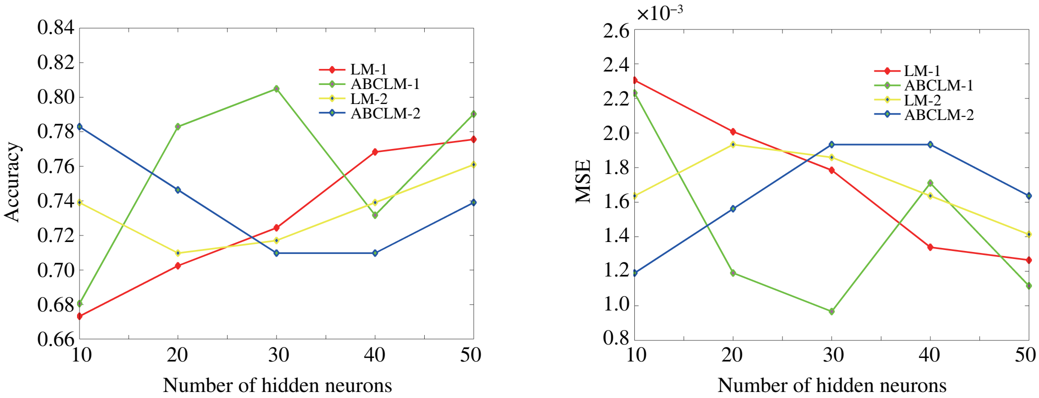
N_H for the comparative analysis. Figure 10 shows the accuracy and MSE for various numbers of clusters. Here, four different variant of proposed algorithms are taken for the performance analysis. LM-1 and LM-2 means that the training was performed using the LM algorithm with 1 and 2 hidden layers. ABCLM-1 and ABCLM-2 means that the training was performed using the ABCLM algorithm with 1 and 2 hidden layers. When analyzing Figure 10(a), the maximum accuracy of 80.49% is achieved by the ABCLM-1 for the cluster size of 2 and 3 and the minimum performance of 70.24% is attained by the LM-2 algorithm. Similarly, MSE graph is shown in Figure 10(b). From Figure 10(b), the best performance (minimum value) of 0.0010 is reached by the ABCLM-1 algorithm for the cluster size of 2 and 3. So, the suggestion here is that the cluster size can be fixed to either 2 or 3 for a better performance in terms of accuracy and MSE.

Figure 11 shows the performance analysis of the proposed detection technique for various numbers of gamma. Here, Figure 11(a) shows the accuracy graph which shows that the better performance is obtained for ABCLM-2 while compared with other variants of the proposed technique. Here, the better performance of 79.76% is obtained by the ABCLM-I when gamma value is fixed to 2.1. The ABCLM-I algorithm obtained the better performance of 77.56% when gamma is fixed to 2.0. When analyzing the four variants of algorithms for different values of gamma, the better performance is mostly obtained either in 2 or 2.1. Similarly, the performance of the proposed detection scheme is analyzed using MSE in Figure 11(b) which is also ensured that the better performance of 0.0010 is obtained for gamma value of 2.1 by the ABCLM-I algorithm. So, the final suggestion is that the better performance can be obtained when gamma is fixed to 2.1.



(a) (b)

Figure 11 (Color online) Various numbers of gamma. (a) Accuracy; (b) MSE.



(a) (b)

Figure 12 (Color online) Various numbers of hidden neurons. (a) Accuracy; (b) MSE.

Figure 12 shows the performance analysis over the various numbers of hidden neurons. Figure 12(a) shows the accuracy graph and Figure 12(b) shows the MSE graph. Here, the better performance for LM-1 is 77.56% when the number of hidden neurons is fixed to 50. The better performance for LM-2 is 76.10% when the number of hidden neurons is fixed to 50. For the ABCLM-1 and ABCLM-2, the better accuracy values are 80.49% and 78.29% when the size of hidden neurons is 30 and 20 respectively. Similarly, in terms of MSE, the better performance of 0.0010 is obtained by ABCLM-1 when the size of hidden neuron is fixed to 30. So, the better performance can be obtained when the hidden neuron size is fixed to 30.

4.3 Comparative analysis

This subsection presents the comparative analysis of the proposed ABCLM and LM algorithm with the existing texture consistence and strength consistence methods given in [9]. For the comparative analysis, the optimal parameters identified from the previous subsection are used here. Then, the size of the training data is varied from 75% to 95% to find the performance deviation of the four algorithms considered. Figure 13(a) shows the accuracy graph of the four methods. From the graph, we understand that the proposed ABCLM outperformed the existing algorithm in all the training data size except 85%. The better performance of 79.76% is reached by the ABCLM algorithm when the training data size is equivalent to 95%. The existing texture and strength of light-based methods achieved only 65.85% and 69.51%. Similarly, comparative results of four algorithms are shown in Figure 13(b) in terms of MSE. This graphs also clearly indicated that the proposed algorithm outperformed the entire existing four algorithms by reaching the minimum value of 0.0010.

Figure 14 shows the comparative analysis of the four algorithms for the different values of radius. Here, radius of texture operator either in LBP or LVP is varied from 1 to 3 and the results are analyzed.

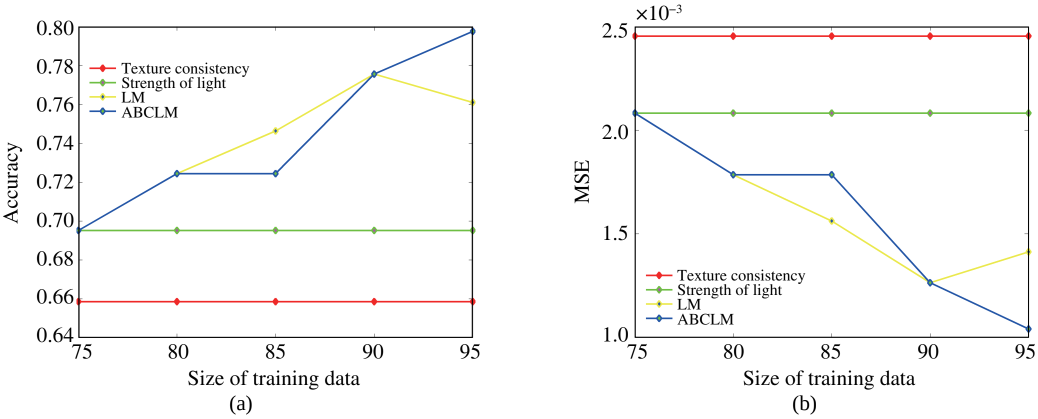


Figure 13 (Color online) Various numbers of training data. (a) Accuracy; (b) MSE.

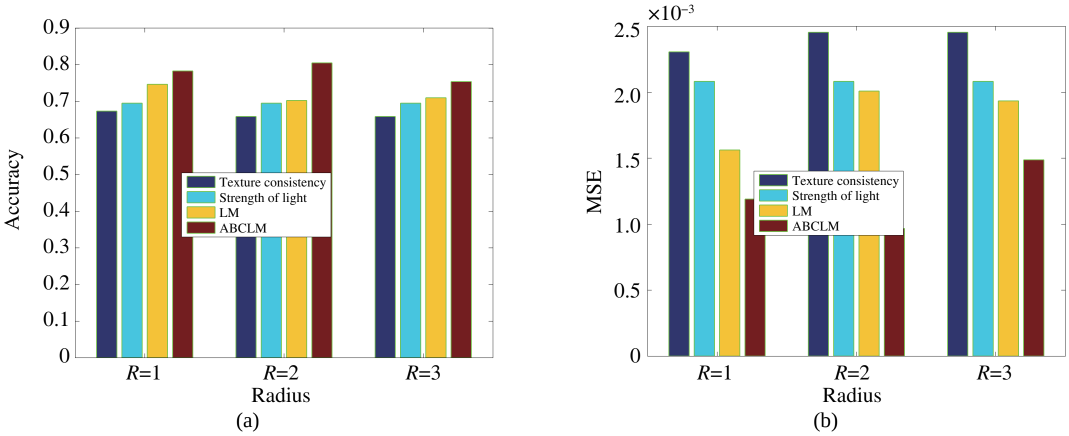


Figure 14 (Color online) Various numbers of texture radius. (a) Accuracy; (b) MSE.

Figure 14(a) shows the performance analysis of four algorithms in terms of accuracy. For the radius of 1, texture, strength of source, LM and ABCLM methods obtained the accuracy of 67.32%, 69.51%, 74.63%, and 78.29% respectively. The better performance of texture, strength of source-based methods and LM algorithm is obtained when the radius size is equivalent to 1. But, the proposed ABCLM obtained the better performance of 80.49% when the radius size is equivalent to 2. Figure 14(b) shows the comparative graphs of the four algorithms in terms of MSE. Here, texture, strength of source, LM and ABCLM methods obtained the MSE of 0.0023, 0.0021, 0.0016 and 0.0012 respectively. The better performance of texture, strength of source-based methods and LM algorithm is obtained when the radius size is equivalent to 1. But, the proposed ABCLM obtained the better performance of 0.0010 when the radius size is equivalent to two. Overall, the proposed ABCLM algorithm obtained better performance for all the different size of radius.

(i) Comparative analysis with various Segmentation algorithms: Figure 15 shows the comparative performance analysis for the true and false positive rate using different number of cluster size. Figure 15(a) represents the performance analysis of true positive rate (TPR). The true positive rate is defined as the proportion measure of positives that are correctly identified. Then, the cluster size is used to segment the images for the digital image forgery. In Figure 15(a), when the size of cluster is four, the existing system like k-means algorithm achieves 84.9% of TPR, 83.67% for GMM segmentation method and DBSCAN attains 83.15% positive rate. But, the proposed FCM method acquires the higher 85.16% of TPR rate compared to the existing system. Thus, the higher value of true positive rate caters the better segmentation performance. Similarly, the performance of false positive rate is represented in Figure 15(b). The FPR measures the proportion of negatives that are correctly identified. The exiting GMM method obtains 17.48%, 19.09%, 16.33%, 16.28%, 19.8% by various number of cluster size. But, the proposed

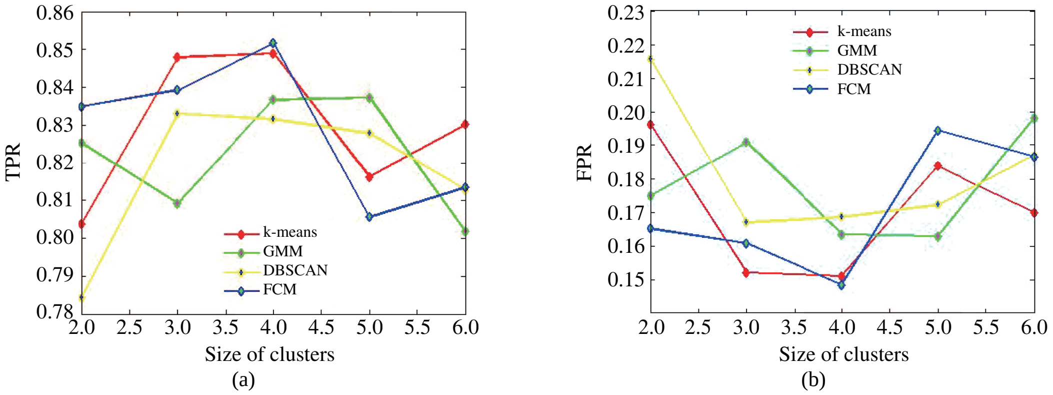


Figure 15 (Color online) Various number of cluster size. (a) TPR; (b) FPR.

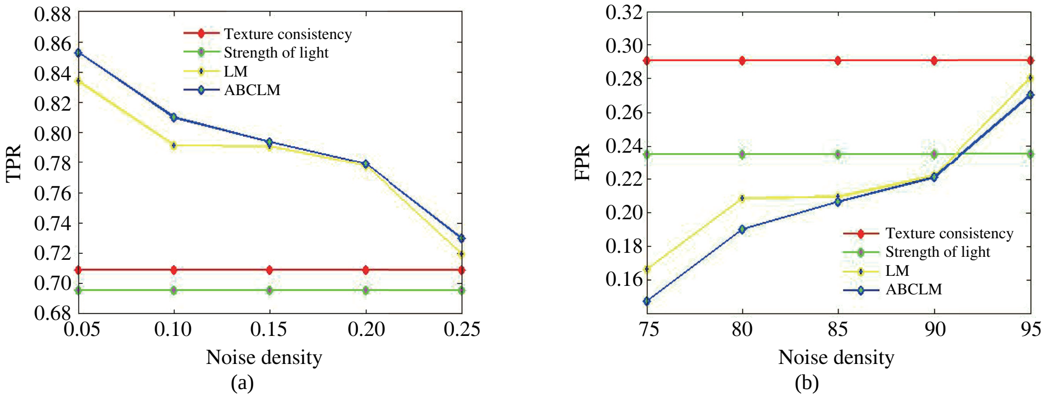


Figure 16 (Color online) Noise density for robustness analysis. (a) TPR; (b) FPR.

FCM achieves the false positive rate of 16.51%, 16.08%, 14.84%, 19.44% and 18.65%. Hence, we infer from Figure 15(b), the lower rate of false positive yields the better accuracy performance.

(ii) Robustness analysis: In general, the performance gets degraded due to noisy regions of the image. But, the proposed system improves the robustness against the noisy pixels. Hence, Figure 16 represents the robustness analysis using the distinct number of noise density level. The robustness is an aspect which improves the performance of the digital image forgery. The TPR performance is shown in Figure 16(a). While using texture consistency, 70.91% true positive rate is obtained for all the noise density level and 69.52% TPR is achieved for strength of light. However, the proposed ABCLM algorithm attains the higher 85.3% true positive when compared to the texture consistency, strength consistency of light source and LM algorithm. Consequently, Figure 16(b) depicts the FPR comparative performance analysis. When the noise density is 85, the existing method acquires 29.09%, 23.48% and 20.9%. Then, the proposed algorithm achieves lower 19% FPR rate. Also, 14.70% false positive is obtained by the proposed ABCLM algorithm when the noise density is 75 compared to the existing systems. Thus, we infer form Figure 16, while increasing the noise density, the higher TPR and lower FPR is obtained compared to the existing system which ensures the robustness of the proposed ABCLM method.

(iii) Color channel: The performance using the three color channel is demonstrated in Figure 17. In general, the color channel poses with three colors such as red, green and blue, used in computer display and image scanners. The Figure 17(a) shows the TPR performance analysis of different color channel. When the performance is analysed by the green channel, the texture consistency and strength of light obtains 70.85% and 69.52%. Thus, we infer that the higher TPR is achieved using proposed algorithm for the three color channel. Subsequently, Figure 17(b) shows the comparative analysis of false positive rate. The Levenberg-Marqaurdt (LM) algorithm achieves 21.45%, 25.52% and 25.61% for red, green and blue color channel. But, the proposed ABCLM algorithm attains 18.79% for red color channel, 16.71% for green color channel and 16.68% for blue color channel when compared to the texture consistency,

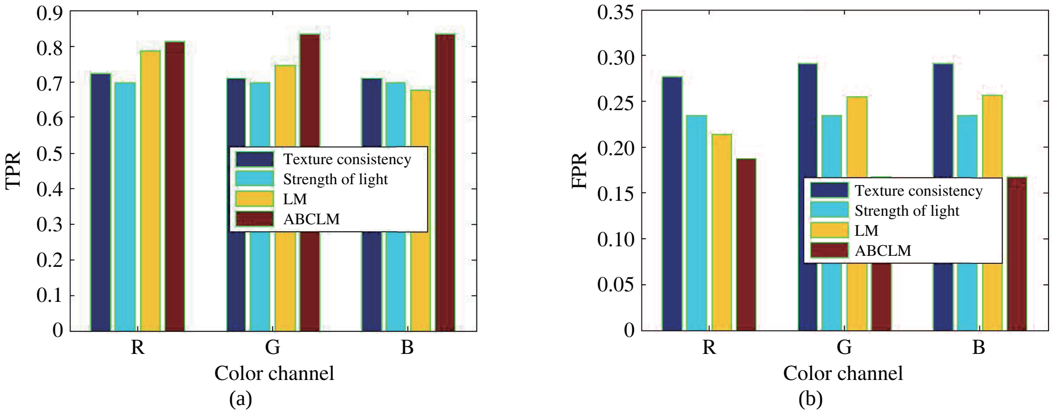


Figure 17 (Color online) Color channel performance. (a) TPR; (b) FPR.

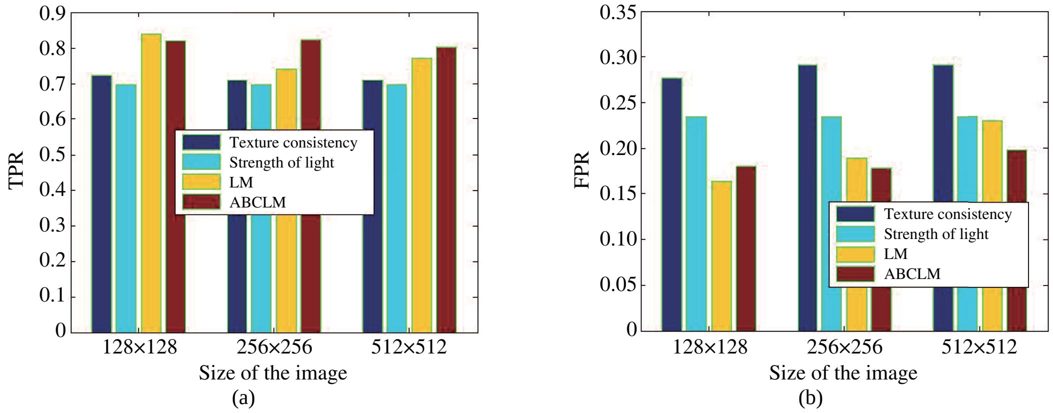


Figure 18 (Color online) Various image size. (a) TPR; (b) FPR.

Table 3 Computation time analysis

Method	Computation time (s)
Texture consistency	44.8
Strength consistency	45.3
LM	32.4
ABCLM	**30.1**

strength of light and LM algorithm. This performance ensured that the proposed method can be able to identify the fraud images for various light source and projections.

(iv) Size of image: The Figure 18 shows the comparative analysis using different number of image size. The TPR comparative performance analysis is shown in Figure 18(a). According to the size of image, the performance is analysed for the existing and proposed method. When the image size is 512 × 512 as input image, the proposed ABCLM algorithm acquires the higher 80.19% TPR value. Comparatively, the proposed algorithm achieves the higher value using different number of image size. Similarly, Figure 18(b) shows the false positive rate performance. The 23.48% FPR is obtained by the strength of light while using the image size is 128 × 128, 256 × 256 and 512 × 512. As compared to the existing system like texture consistency, strength of light and LM algorithm, the ABCLM algorithm attains the lower false positive rate. Thus, the lower 17.89% FPR is obtained which improves the accuracy performance.

(v) Computation time: Table 3 explains the computational time analysis for the existing and proposed method. It is defined as the measure of time required to perform the forgery detection using consistent feature and fuzzy based segmentation. Compared to the exiting method, the proposed ABCLM method attains the low computation time 30.1 s which reduces the computation complexity of the system.

5 Conclusion

We have proposed a technique for image forgery detection either in shadow or reflection using consistency features and fuzzy-based segmentation. Here, shadow regions were extracted using shadow map-based segmentation and the reflective points were extracted using fuzzy c-means clustering. Once shadow and reflective points were identified, LVP-based texture pattern was extracted and the strength of light source was estimated using mean, standard deviation, kurtosis and correlation co-efficient. The features extracted from the images were then given to the neural network to detect whether the input image is forgery or authenticated shadow or reflection. Here, neural network was trained with the proposed learning algorithm, ABCLM which combines the LM and ABC algorithm. The experimentation is performed with the dataset collected from the public resources and the evaluation of the proposed forgery detection is performed using two parameters, such as accuracy and Mean Square Error. From the outcome, we proved that the proposed ABCLM obtained the better performance of 80.49% when compared with other techniques, such as texture, strength of source and LM-based techniques which were obtained the accuracy of 67.32%, 69.51% and 74.63% respectively.

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Muhammad G, Hussain M, Bebis G. Passive copy move image forgery detection using undecimated dyadic wavelet transform. Digit Investig, 2012, 9: 49–57

2 Muhammad G, Hussain M, Khawaji K, et al. Blind copy move image forgery detection using dyadic undecimated wavelet transform. In: Proceedings of 17th International Conference on Digital Signal Processing (DSP), Corfu, 2011. 1–6

3 Birajdar G K, Mankar V H. Digital image forgery detection using passive techniques: a survey. Digit Investig, 2013, 10: 226–245

4 Kee E, O'Brien J F, Farid H. Exposing photo manipulation from shading and shadows. ACM Trans Graph, 2014, 33: 165

5 Zhang W, Cao X C, Zhang J W, et al. Detecting photographic composites using shadows. In: Proceedings of the IEEE International Conference on Multimedia and Expo, New York, 2009. 1042–1045

6 Liu Q G, Cao X C, Deng C, et al. Identifying image composites through shadow matte consistency. IEEE Trans Inform Forens Secur, 2011, 6: 1111–1122

7 Yang B, Sun X M, Chen X Y, et al. Exposing photographic splicing by detecting the inconsistencies in shadows. Computer J, 2015, 58: 588–600

8 Ge H Y, Malik H. Exposing image forgery using inconsistent reflection vanishing point. In: Proceedings of International Conference on Audio, Language and Image Processing, Shanghai, 2014. 282–286

9 Ke Y Z, Qin F, Min W D, et al. Exposing image forgery by detecting consistency of shadow. Sci World J, 2014, 2014: 364501

10 Bayram S, Sencar H T, Memon N. An efficient and robust method for detecting copy-move forgery. In: Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing. Washington DC: IEEE Computer Society, 2009. 1053–1056

11 Popescu A C, Farid H. Exposing digital forgeries by detecting traces of re-sampling. IEEE Trans Signal Process, 2005, 53: 758–767

12 Wang W, Dong J, Tan T N. Effective image splicing detection based on image chroma. In: Proceedings of IEEE International Conference on Image Processing, Cairo, 2009. 1257–1260

13 O'Brien J F, Farid H. Exposing photo manipulation with inconsistent reflections. ACM Trans Graph, 2012, 31: 4

14 Rufenacht D, Fredembach C, Susstrunk S. Automatic and accurate shadow detection using near-infrared information. IEEE Trans Patt Anal Mach Intell, 2013, 36: 1672–1678

15 Fan K-C, Hung T-Y. A novel local pattern descriptor—local vector pattern in high-order derivative space for face recognition. IEEE Trans Image Process, 2014, 23: 2877–2891

16 Hagan M T, Menhaj M. Training feed-forward networks with the Marquardt algorithm. IEEE Trans Neural Netw, 1994, 5: 989–993

17 Karaboga D, Basturk B. A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm. J Global Optim, 2007, 9: 459–471

18 Kee E, O'Brien J F, Farid H. Exposing photo manipulation with inconsistent shadows. ACM Trans Graph, 2013, 32: 28

19 Cao X C, Zhao H D, Wang C, et al. Image composite authentication using a single shadow observation. Sci China Inf Sci, 2015, 58: 092110

20 Otsu N. A threshold selection method from gray-level histograms. IEEE Trans Syst Man Cybern, 1979, 9: 62–66

21 Bezdek J C. Pattern Recognition with Fuzzy Objective Function Algorithms. New York: Plenum Press, 1981

22 Auer P, Burgsteiner H, Maass W. A learning rule for very simple universal approximators consisting of a single layer of perceptrons. Neural Netw, 2008, 21: 786–795