Wireless Pers Commun (2018) 98:3039–3057
https://doi.org/10.1007/s11277-016-3941-1

Non-intrusive Forensic Detection Method Using DSWT with Reduced Feature Set for Copy-Move Image Tampering

V. Thirunavukkarasu[1] · J. Satheesh Kumar[1] · Gyoo Soo Chae[2] · J. Kishorkumar[3]

Published online: 6 January 2017

Abstract The key intention of non-intrusive image forensic detection is to resolve whether an image is original or tampered. In contrast to intrusive methods, there is no supporting pattern that has been embedded into an image to ensure image authenticity. The only accessible cue is the original characteristics of an image. Various non-intrusive techniques have been proposed to ensure image authenticity but no adequate solution exists so far. This article introduced a robust technique by means of Discrete Stationary Wavelet Transform along with Multi Dimension Scaling to detect familiar category of copy-move image tampering. Experimental outcomes shows that proposed technique decreases computational complexity by reducing feature dimension and locate the tampered region more accurately even when the tampered image is blurred, brightness altered, colour reduced and pasted in multiple locations. Overall tamper detection accuracy is greater than 97% and false positive rate close to zero, which indicates that proposed technique will discover tampered region more precisely compared with existing methods.

Keywords Intrusive · DSWT · MDS · Copy-move · Tampering · Blurring

✉ J. Satheesh Kumar
jsathee@rediffmail.com

V. Thirunavukkarasu
arasu_mca3@yahoo.com

Gyoo Soo Chae
gschae00@gmail.com

J. Kishorkumar
sharkishor@rediffmail.com

[1] Department of Computer Applications, School of Computer Science and Engineering, Bharathiar University, Coimbatore, Tamil Nadu, India

[2] Division of Information and Communication, Baekseok University, Cheonan, South Korea

[3] Department of Physics, Arignar Anna Government Arts College, Cheyyar, Tamil Nadu, India

1 Introduction

Digital image tampering is not a difficult task owing to the rapid growth of dominant image manipulation software's and practices. It does not require any professional skills or training hence, an average user can perform it without leaving any visual cues. Images are manipulated for various reasons and some manipulations are performed with precise intention to deceiving a court, public or forgery. Other manipulations are performed without any explicit intension such as entertainment or marketing products [1, 2]. There exists different ways to counterfeit the content of an image. Copy-move, image compositing and retouching are most common techniques of forgery [3]. Image splicing employs assortment, renovation and merging of image area's for structuring spliced image. Unlike image splicing, image retouching is not as much of impairment. Instead of altering the content of an image, retouching can increase or decrease certain features in the image. This technique is most popular with magazine picture editors to project their wrapper images [4]. Copy-move is familiar image tampering technique where specific region in the image is copied as well as inserted at different area of an image as shown in Fig. 1 [5].

It is essential to ensure the genuineness of image content when it is used as evidence. Developing an automatic tamper detection algorithm to ensure trustworthiness of an image is most prominent research area in image processing [6]. Many techniques have been proposed to authenticate image content that are categorized into two types such as intrusive and non-intrusive techniques. In intrusive technique, digital watermark or digital signature is implanted for ensuring integrity of an image [7]. The user specified algorithms are used in non-intrusive techniques for source identification and tamper detection. Source identification is a process of identifying imaging devices such as digital camera, digital scanner, mobile phone or medical imaging devices. Imaging devices can be identified in the presence of lens radial distortion, sensor noise, pixel defects and color filter array (CFA) interpolation.

Tamper detection is achieved by checking inconsistencies in camera characteristics, physical environment and image manipulation. Non-intrusive Image forensics detection is comparatively a new research direction in forensic domain. The proposed algorithm is introduced to discover tampered image region with high accuracy and low false positive rate even the tampered region is distorted. The potential application of image tamper detection has higher influence in different domains such as forensic investigation, law enforcement, scientific journals and insurance claim processing [8].

2 Copy-Move Tamper Detection Methods-A View

Numerous non-intrusive forensic methods for copy-move tamper discovery are proposed during last decade. These techniques were separated with block oriented and key point oriented techniques [9, 10]. In block oriented methods, suspected image is alienated with overlapping and non-overlapping sub-blocks and feature vectors were retrieved to match its nearest neighbor. However, key point based methods identify key points with high entropy image regions as well as matching key point features to locate tampered region. It outperforms block based method when the tampered region is affected by geometric or illumination distortion. Fridrich et al. introduced familiar technique through Discrete Cosine Transform (DCT) coefficients for fixed size image blocks. This method was efficiently discovers copy-move tampered region even it is enhanced or retouched however,

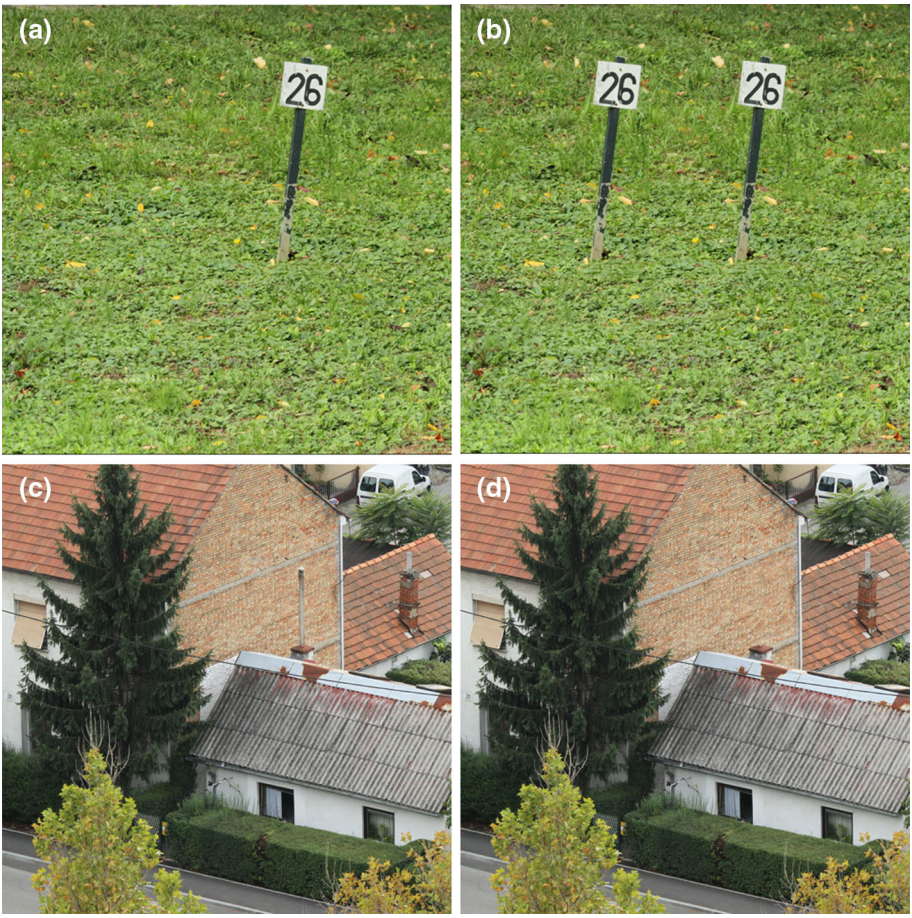

Fig. 1 Illustration of copy-move tampering. **a**, **c** Authentic images, **b** tampered image with duplicated region, **d** tampered image which conceal one object

the algorithm did not carry out any other robustness test and dimension of feature vectors leads higher computational complexity [11].

Popescu et al. make use of Principle Component Analysis coefficients to obtain condensed dimension depiction of image blocks. Accuracy of this technique is high compared with previous methods however, the method is inappropriate to the images with stumpy JPEG qualities and small image blocks [12]. Mehdi et al. introduced a technique by means of Discrete Wavelet Transform (DWT) and DCT Quantization Coefficients for recognizing tampered region of an image. This approach reduced the feature dimension as 16 to improve computational speed but it fails to detect tampered region with some geometric transformations [13]. Zhao et al. presented a technique with respect to DCT and Singular Value Decomposition (SVD) to represent image segments. This technique diminish the computational complexity by reducing feature dimension and successfully detects multiple copy-move regions even though it was contaminated by Additive White Gaussian Noise (AWGN), JPEG compression along with its mixture operation. Accuracy was degraded while Signal to Noise Ratio is more than 45 db and JPEG quality factor is below 70% [14].

Bravo et al. used log polar transformation by mapping the Cartesian space coordinates into radius(r) and angle θ (theta) relative to the origin of coordinate system. This procedure enormously reduces the size of feature vector used in block matching phase and suitable to detect tampered region with rotation and scaling however, it is not appropriate for tampered image with additive noise, blurring and JPEG compression [15].

Cao et al. developed a circle block method. In which every DCT coefficient square blocks are transformed into a circle block to reduce feature dimensionality. Feature descriptors were lexicographically arranged and matched with threshold value. This technique is efficient to perceive multiple copy-move regions as well as the copy-move region with blurring and noise distortion but it is not appropriate to detect copy-move tampering with some basic geometric operations [16]. Cheng et al. employed a robust technique to detect copy-moved and in-painted tampered images. Suspected image regions are discovered by comparing similarity between blocks and tampered regions are located with multi-region relation model. Weight transformation based searching algorithm was deployed to enhance the computation speed. This approach fails in situation where the tampered region is too small and distressed by blurring [17]. Leida et al. projected an efficient scheme in the direction of perceiving a tampered area which is rotated or scaled. Suspected image was separated to circular blocks as well as feature descriptors were retrieved by polar harmonic transform. Feature matching is performed by lexicographical sorting and tampered regions are marked by identifying similar circular blocks [18].

Li et al. presented a technique by means of DWT and SVD to distinguish tampered image with original. This process decreases computational complexity but not succeeded to detect the tampered region which is blurred or flipped [19]. Yang et al. implements an efficient method through Discrete Wavelet Transform and Fast Walsh-Hadamard Transform. Tamper detection time is successfully reduced compared with other methods but it is not efficient to detect the tamper region which is distressed with some geometric transformation attacks [20]. Lee et al. deployed a method based on Histogram Oriented Gabor Magnitude (HOGM) to discover and localize the copy-move tampering. Noise detector method is developed with the intension of reducing false matches. Euclidean distance is employed to match tampered region. This technique is robust against various image deformation operations like rotation, resizing, JPEG compression, blurring and brightness change [21].

3 Role of DSWT and MDS in Tamper Detection

Wavelet transformation is employed to view or process the image at multiple resolution through which different frequencies are examined with different resolutions. In contrast to Fourier transform that reveals only frequency characteristics, wavelet transform reveals both frequency and spatial characteristics of an image. It decompose an image into approximate and detail sub bands.

3.1 Discrete Stationary Wavelet Transform (DSWT)

Most of the existing method uses DWT in support of copy-move tamper discovery. However, DWT is non shift invariant descriptor since it entailed down sampling and produce blurring along with noise in the edge regions. To overcome the above drawback DSWT is proposed which is shift and time invariant in nature. For example, while

performing copy–move tampering the tampered regions may possibly situated at different locations in two blocks (refer Fig. 2), the non-shift invariant descriptor produce two different representations and fails to notice tampered region. Conversely, shift invariant descriptors like DSWT treated these blocks are similar. DSWT have identical number of coefficients at every levels and suitable for edge recognition, de-noising and pattern recognition. The approximate and detailed coefficients of DSWT at a particular level j for an R × C input image can be obtained using the formula,

$$A_j[R, C]=\left(lf^j lf^j * a_j\right)[R,C] \tag{1}$$

$$H_j[R, C]=\left(lf^j hf^j * a_j\right)[R,C] \tag{2}$$

$$V_j[R, C] = \left(hf^j lf^j * a_j\right)[R, C] \tag{3}$$

$$D_j[R, C] = \left(hf^j hf^j * a_j\right)[R,C] \tag{4}$$

where *A*, *H*, *V*, *D* are the approximate, horizontal, vertical and diagonal coefficients respectively and hf, lf represents high and low pass filters. Size of the 2D image is represented as R × C [22]. Figure 3 illustrates how DSWT is applied to 2D image.

3.2 Multi Dimensional Scaling (MDS)

MDS provides visual representation of similarities or dissimilarities among the set of data items. It is a classical approach to perform dimensionality reduction by transforming higher dimensional data into lower dimensional representation by retaining distance between data points. For example given m data items in a q-dimensional space, MDS generates k-dimensional representations of the data items such that $k \leq q$. It provides analytical solution without requiring any iterative procedure. Euclidean distance is used to measure similarities or dissimilarities among the data items. If the distance is small then the data items are similar otherwise dissimilar. MDS is widely used to discover hidden structure, data visualization in fMRI analysis and molecular modelling. For a given input matrix, the proximities between every pair of data items $P = [d_{pq}]$ is computed using the formula,

$$d_{pq}=\sqrt{\left(x_p - x_q\right)^2+\left(y_p - y_q\right)^2} \tag{5}$$

where d_{pq} represent distance among pth and qth data item. The coordinate matrix C can be derived by Eigen value decomposition with the following procedure.

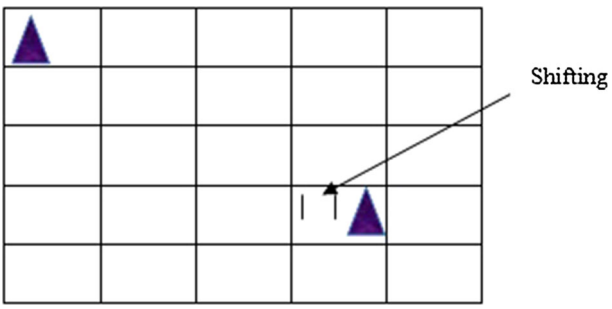

Fig. 2 Example for shifting in copy-move forgery

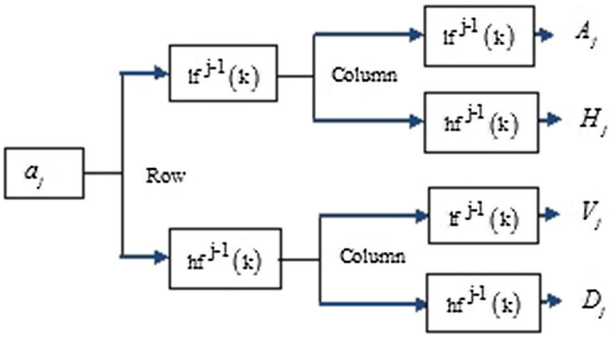

Fig. 3 DSWT decomposition of 2D image at level one

Algorithm:

Step 1 Set up the squared proximity matrix $p^2 = d_{pq}^2$

Step 2 Scalar product matrix *S* can be constructed from the proximity matrix *P* using the formula,

$$S = -\frac{1}{2} QP^2Q \tag{6}$$

Matrix Q is calculated with double centring method, $Q = I - nd^{-1}\tilde{I}$, where I is a unit matrix, $\tilde{I}$ indicate matrix of ones and nd represents number of data items.

Step 3 Extract m largest Eigen values $e_1 \ldots e_m$ of S and the corresponding Eigen vectors $V_1 \ldots V_m$

Step 4 The m dimensional organization of n items are obtained from the coordinate matrix

$$C = V_m D_m^{1/2} \tag{7}$$

where V_m is a matrix with m Eigen vectors moreover, D_m illustrate diagonal matrix with m Eigen values of S. Degree of correspondence between data items implied by MDS map and input matrix is expressed by two metrics such as stress function and Sammon cost function. Stress function is represented as

$$f(y) = \sum_{i,j} (||h_i - h_j|| - ||l_i - l_j||)^2 \tag{8}$$

where the value of f(y) shows degree of correspondence among low and high-dimensional representation of data, $||h_i - h_j||$ indicates Euclidean distance among high dimensional data points h_i and h_j. Euclidean distance among low dimensional data points l_i and l_j is $||l_i - l_j||$. Sammon cost function is varying from stress function where it put more importance to hold the distances that were originally small. It is calculated using the formula,

$$\rho(Y) = \frac{1}{\sum_{i,j} \|h_i - h_j\|} \sum_{i^1 j} \frac{\left(\|h_i - h_j\| - \|1_i - 1_j\|\right)^2}{\|h_i - h_j\|} \tag{9}$$

where $\rho(y)$ holds minimum distance data points [23].

4 Proposed Tamper Detection Approach

The proposed method employs Discrete Stationary Wavelet Transform (DSWT) to segregate suspected image at various frequency bands such as LL, LH, HL and HH at level one. Out of four different bands LL is better for tamper detection since it contains all approximate coefficients of input image. Multi Dimensional scaling (MDS) is deployed for diminishing dimension of feature descriptors. Similarities between the blocks are identified with lexicographical sorting, finally tampered region is located.

4.1 Proposed Approach

The proposed non-intrusive forensic discovery procedure is exposed in Fig. 4. Entire algorithm structure involves six steps: (1) Converting color image into intensity image (2) Applying DSWT to preprocessed image (3) Extract LL sub-band and divide it into overlapping blocks (4) Applying multi dimensional scaling to decrease feature dimension (5) Match features vectors using lexicographical sorting and (6) Localize the tampered region.

Algorithm

Step 1 Input color image is preprocessed by the equation,

$$\mathrm{LC} = 0.299\,R + 0.587\,G + 0.114\,B \tag{10}$$

In the above equation *R*,*G* and *B* indicates three color components and *LC* is the luminance component of input image.

Step 2 Discrete Stationary Wavelet Transform (DSWT) is applied to preprocessed input image at level one.

Step 3 The approximate coefficients (LL) of DSWT has been extracted, since it contains most of the image information than the detailed coefficients (LH, HL, and HH). Comparing every pixel with all other pixels leads higher computational complexity thus the suspected image is separated with overlapping blocks of stipulated size BS × BS. For a given input image of size R × C, total blocks should be (R − BS + 1) (C − BS + 1). Where R and C indicate number of rows and columns respectively and BS represents block size.

Step 4 To reduce the feature dimension, MDS is applied to each overlapping block of size 8 × 8.

Step 5 Reduced feature vectors are stored in a two dimensional matrix CA of (R − BS + 1) (C − BS + 1) rows with 8 columns, subsequently the algorithm stores position of two rows if they are identical and shift vector S is calculated using the formula,

$$S = ||i_1 - j_1,\, i_2 - j_2|| \tag{11}$$

where i_1,i_2 and j_1, j_2 indicates the positions of identical rows. To remove false matches the proposed algorithm employs threshold value. When the shift vector occurrence exceeds the threshold value then only the blocks are considered as tampered.

Fig. 4 The proposed framework

5 Experimental Results

5.1 Data Set

Tamper detection performance of proposed technique is assessed with two different publically available data sets designed for unrestricted research usage. First dataset includes 24 true uncompressed color images with 768 × 512 pixels launched by Kodak Corporation [24]. Moreover the second one is CoMoFoD data set which consists of 200 color images with dimension 512 × 512 introduced by video communication laboratory [25].

5.2 Performance Evaluation

Performance of proposed technique is assessed by means of two evaluation criteria such as Accuracy Rate (AR) and False Positive Rate (FPR) which is determined using the formula,

$$AR = \frac{TP + TN}{TP + TN + FN + FP} \tag{12}$$

In the above equation, TP indicates true positive which designates amount of tampered pixels that are accurately categorized as tampered. The amount of genuine pixels that are rightly classified as such is measured by true negative (TN). Metric FP refers false positive which measures fraction of genuine pixels that are categorized with tampered. FN specifies false negative which indicates amount of tampered pixels that is categorized as original. AR value indicates how accurate the proposed algorithm locates pixels of copy-move tampered region. False positive rate is calculated with the formula,

$$FPR = \frac{FP}{FP + TN} \tag{13}$$

where FPR indicates the amount of pixels that are not included in tampered area however; it is erroneously incorporated with proposed technique. If the value of AR and FPR is closer to 1 and 0 respectively then the detection method has high accuracy.

5.3 Efficiency and Accuracy Test

To exhibit efficiency and accuracy of proposed scheme 24 color images of size 768 × 512 were selected from the first data set and 40 source images of size 512 × 512 were selected from the second data set. Test images used in this experiment does not require any post processing operations. Due to space constraint, simply a few experimental outcomes were shown here. Proposed technique effectively identify the simple and multiple non-regular copy-move tampered areas even the tampered region is too small. Figure 5 illustrate the detection result of non-regular copy-move tampering. Detection outcome of multiple region tampering is exposed at Fig. 6.

Detection result reveals that the proposed technique successfully detects tampered image even it has multiple copy-move regions. The statistical detection rate of proposed method is evaluated under two different data sets. Experimental results shows that Accuracy Rate (AR) is greater than 0.9 and false positive rates (FPR) are near to 0. This shows that the proposed scheme more precisely locating tampered region.

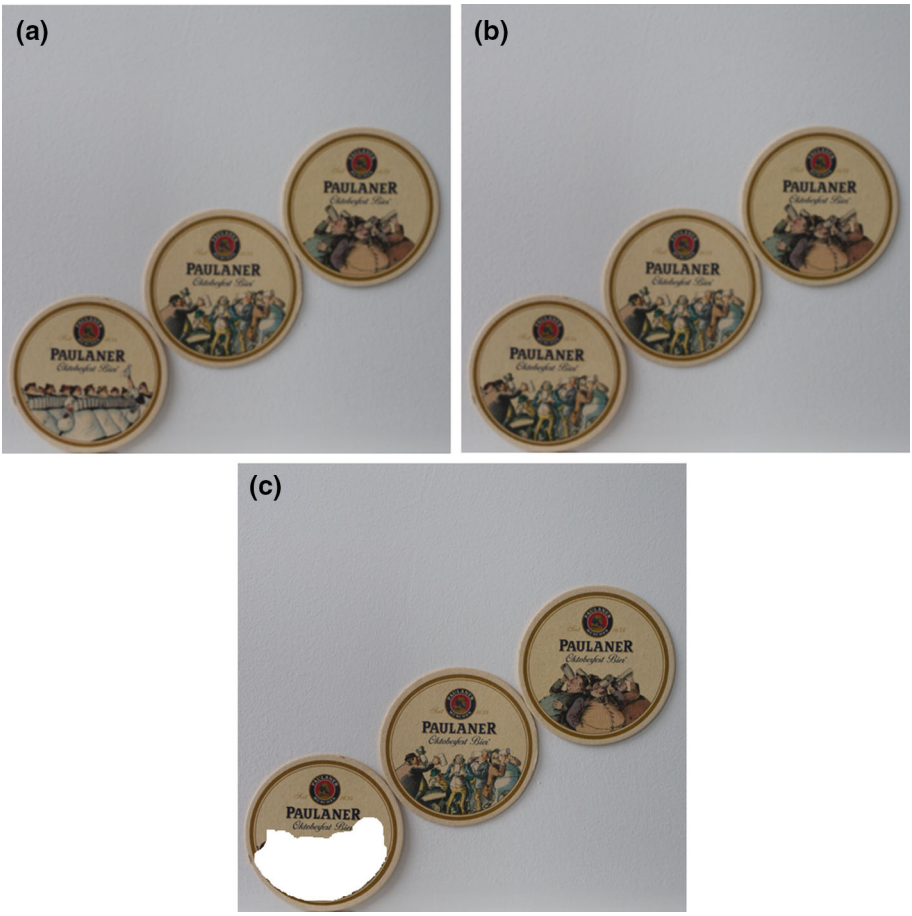

Fig. 5 **a** Authentic image, **b** manipulated image, **c** discovered outcome, AR/FPR rates are 0.9845/0.0126

5.4 Robustness Test

5.4.1 Robustness Against Blurring

Numerous alterations are made with tampered images, blurring is frequently applied technique towards to cover traces of tampering. In this section robustness of proposed algorithm is evaluated under different blurring conditions. CoMoFoD database is employed for this purpose which contains 120 tampered images (Image No. 001_F_IB1 to 040_F_IB3) blurred through three dissimilar averaging filters (3×3, 5×5 and 7×7). Figure 7 shows the tampered image blurred with 5×5 averaging filter and its discovered outcome. Table 1 demonstrates the empirical outcome of 120 forged images with three different averaging filters. Proposed algorithm attains high accuracy and low false positive rate when tampered images are blurred with 3×3 and 5×5 averaging filter. However, detection performance fall under 7×7 averaging filter.

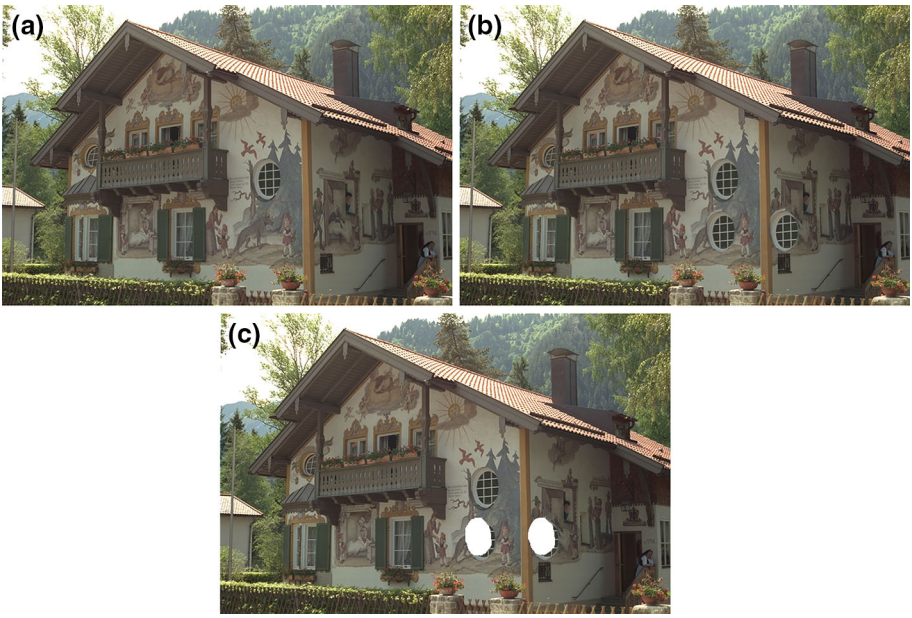

Fig. 6 **a** Authentic image, **b** manipulated image, **c** discovered outcome, AR/FPR rates are 0.9897/0.007

5.4.2 Robustness Against Brightness Change

Tampered images are distorted with brightness change by mapping the intensity values of forged image in the interval [0 1]. Intensity values below and above this intervals are saturated to minimum and maximum values, as a result three different ranges of brightness such as (0.01, 0.95) (0.01, 0.9) and (0.01, 0.8) were created. Kodak image data set does not include tampered image distorted by brightness change or color reduction hence, CoMoFoD database is employed in this purpose. Figure 8 shows tampered image with brightness altered in the range (0.01, 0.9) and corresponding detection result.

Average detection performance of 120 tampered images (Image:001_F_BC1 to 040_F_BC3 in the CoMoFoD database)with various ranges of brightness altered is listed in Table 2. AR and FPR values indicates that the proposed method exhibit excellent robustness against tampered image with different ranges of brightness change.

5.4.3 Robustness Against Colour Reduction

In addition to handling blurring and brightness change proposed method is also capable of handling forged images which are deformed with colour changes. Colour diminishing is performed by consistent quantization of image pixel values [27]. In every colour channels of tampered image pixel values are diminished from the level 256–32, 64 or 128. Figure 9 is an example for forged image by colour reduced at level 64 as well as its equivalent discovered outcome.

In the direction of estimating performance of proposed technique CoMoFoD database is employed. This include 120 tampered images (Image: 001_F_CR1 to 040_F_CR3) which were distorted by color reduction at three different levels. Table 3 exposed that the proposed technique achieved high accuracy rate (AR) and low false positive rate (FPR) even the tampered images are distorted by different color reduction levels.

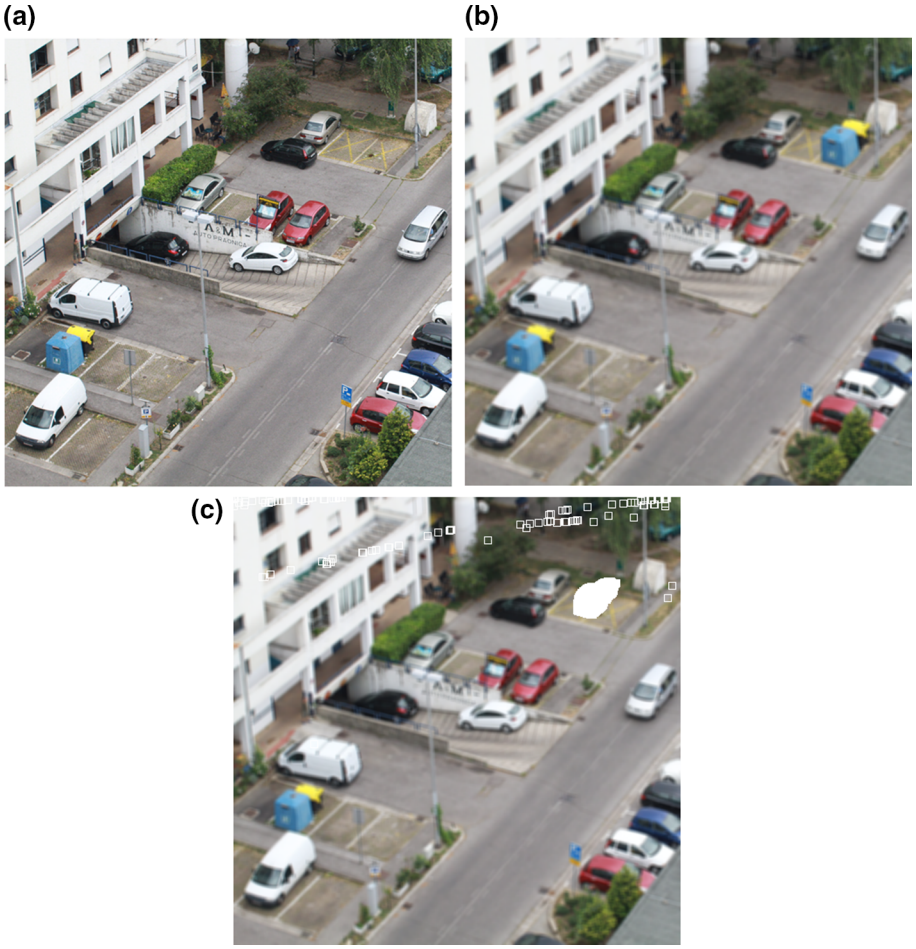

Fig. 7 **a** Authentic image, **b** tampered image blurred by 5 × 5 averaging filter, **c** detection result

Table 1 Detection performance against forged images deformed with Gaussian blurring

Metric	Blurring with different Average filter			Average performance
	3 × 3	5 × 5	7 × 7	
AR	0.9851	0.9801	0.9523	0.9725
FPR	0.0152	0.0415	0.0651	0.0406

5.5 Comparisons with Existing Methods

5.5.1 Computational Complexity

The computational complexity is a significant problem to any non-intrusive tamper detection algorithm. It is examined against state of art approaches by means of feature

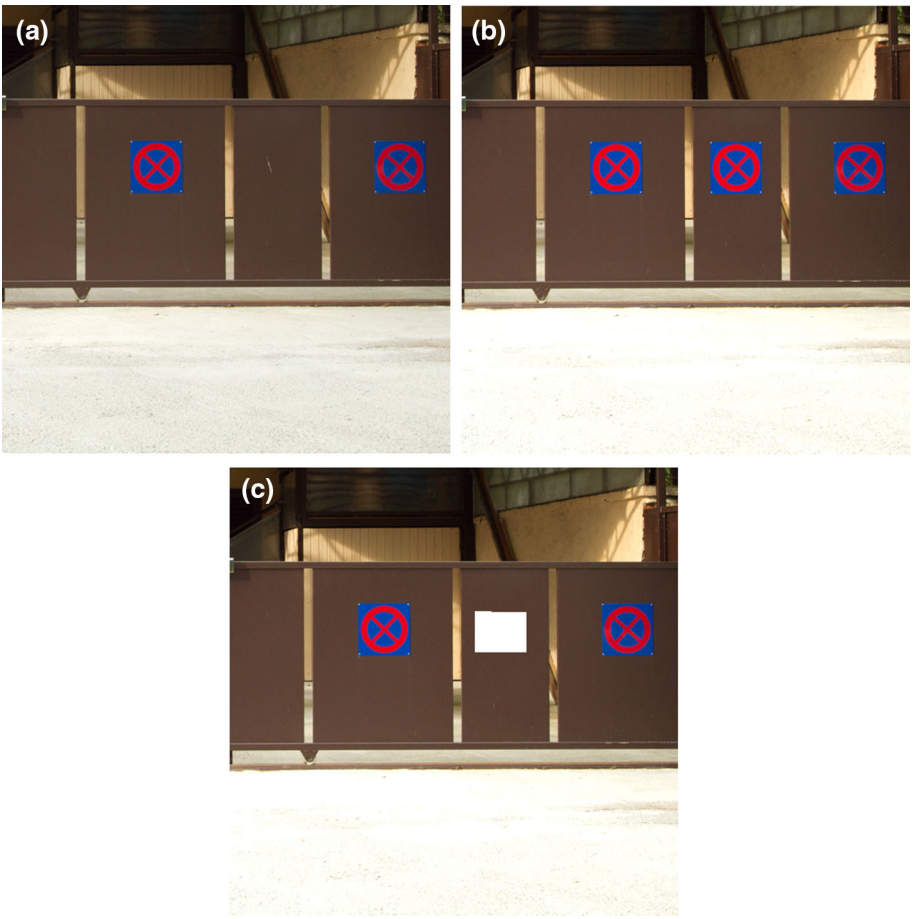

Fig. 8 **a** Authentic image, **b** tampered image with brightness altered range (0.01, 0.9), **c** discovered outcome

Table 2 Detection performance against forged images distorted by brightness change

Metric	Brightness adjustment range			Average performance
	(0.01,0.95)	(0.01,0.9)	(0.01,0.8)	
AR	0.9871	0.9856	0.9791	0.9839
FPR	0.0119	0.0120	0.0180	0.0139

dimension. The suspected image is alienated with overlapping blocks with size 8×8 to extract DSWT feature descriptor and MDS is applied to every block to reduce its feature dimension. Every block coefficients are accumulated in a single row of two dimensional matrix CA. Number of rows in the matrix represent total blocks and number of columns specifies feature dimension. Before applying dimensionality reduction method, 64 features have used to represent each block. After applying dimensionality reduction method, 8 features have been used to represent each block. Table 4 illustrates the comparison result of feature dimension.

Fig. 9 **a** Authentic image, **b** forged image with colour depth diminished to level 64, **c** detection result

Table 3 Detection performance against tampered images distorted by color reduction

Metric	Color reduction levels			Average performance
	32	64	128	
AR	0.9835	0.9897	0.9920	0.9884
FPR	0.0180	0.0109	0.0106	0.0131

5.5.2 Detection Performance

Detection outcome of proposed technique is examined among existing methods by means of Accuracy Rate (AR) and False Positive Rate (FPR). Data set images used by Zhao et al. [14] and Lee et al. [21] were utilized to assess detection performance. Images in Fig. 10 used by Zhao et al. are tested by proposed technique and discovered outcomes are

Table 4 Feature dimension comparison with existing algorithms

Method	Algorithm	Feature dimension
Fridrich et al. [11]	DCT	64
Popescu et al. [12]	PCA	32
Zhao et al. [14]	DCT & SVD	16
Lee et al. [21]	HOGM	12
Proposed Method	DSWT & MDS	8

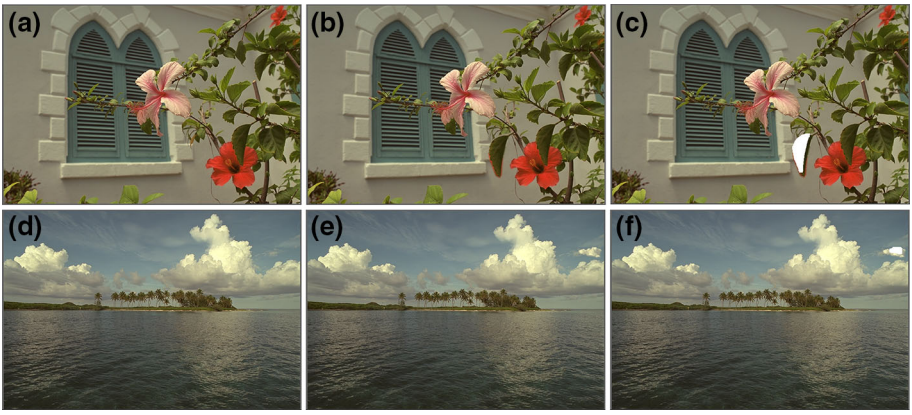

Fig. 10 **a**, **d** Authentic images, **b**, **e** forged images, **c**, **f** detection result of proposed method

displayed. Similarly images in Fig. 11 used by Lee et al. are tested and discovered outcomes are displayed.

Performance of proposed technique is evaluated with Zhao et al. [14] and Lee et al. [21] methods and resultant values are given in Table 5. It illustrate that Accuracy Rate (AR) of proposed technique is above 0.95 and False Positive Rates (FPR) are close to 0. This indicates that the proposed technique discover tampered region exactly even though the tampered regions are too small and non- regular.

Figure 12 demonstrates the performance assessment curves of proposed method with existing well known techniques namely Fridrich et al. [11], Popescu et al. [12] and Lee et al. [21] under different image distortion like blurring, brightness change and color reduction. AR curve in Fig. 12a, demonstrate that the proposed technique outperforms other techniques for tampered images blurred with different averaging filters. FPR curve in Fig. 12b reveals that the proposed method provides lower FPR values even the tampered images is blurred with 7×7 averaging filter. Figure 12 c, d shows the comparison result of tampered images with brightness change in three different levels (0.01, 0.9) (0.01, 0.95) and (0.01, 0.8). Raising brightness level leads to increase the AR value and reduce the FPR value in all four methods. AR and FPR curves of proposed method exhibit good performance than the existing methods. Figure 12e, f displays the comparison outcome of forged images deformed with colour reduction in three different intensity levels (32, 64 or 128). Efficiency of proposed technique improves at higher intensity level changes than the lower level changes [26].

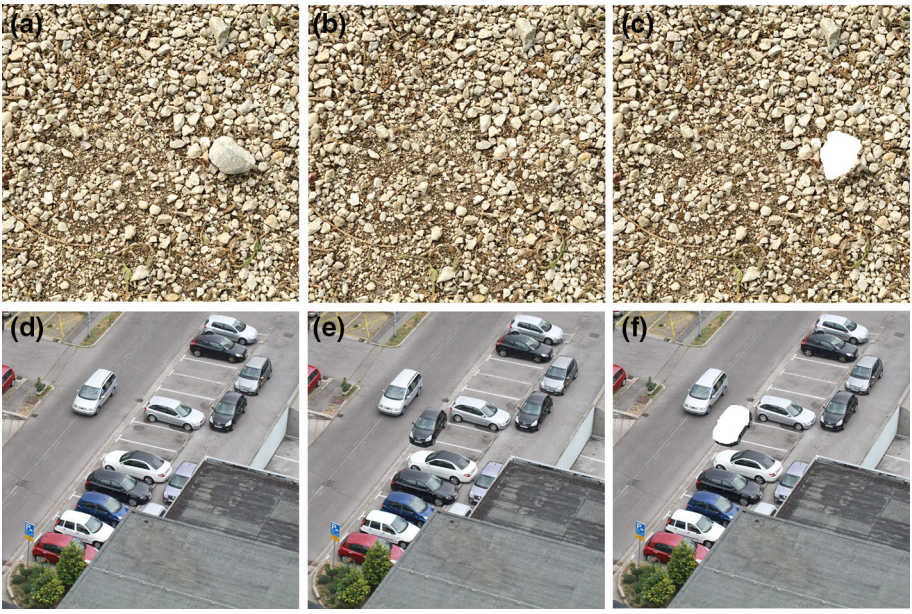

Fig. 11 **a**, **d** Authentic images, **b**, **e** forged images, **c**, **f** detection result of proposed method

Table 5 Detection result of tampered images using proposed method, Zhao et al. [14] and Lee et al. [21] methods

Image	Existing methods	Performance of existing method		Performance of proposed method	
		AR	FPR	AR	FPR
Figure 8(b)	Zhao et al. [14]	0.949	0.002	0.995	0.0006
Figure 8(e)	Zhao et al. [14]	0.872	0.013	0.971	0.012
Figure 9(b)	Lee et al. [21]	0.974	0	0.986	0
Figure 9(e)	Lee et al. [21]	0.982	0	0.995	0

6 Conclusion

In this article a robust non-intrusive forensic detection technique using DSWT and MDS is proposed. DSWT and MDS feature descriptors can automatically identify copy-move tampered region without the knowledge of image content. The algorithm use less features to characterize all block. Empirical outcome shows that the proposed technique not merely discover forged area which is too small and non-regular but also has strong robustness to detect multiple tampered region and tampered region distorted by blurring with different average filter, brightness and color reduction at different levels. Compared with state of art techniques, proposed technique has less computational difficulty and high accuracy. This effort makes valuable contribution in image forensic detection. Reliable method that

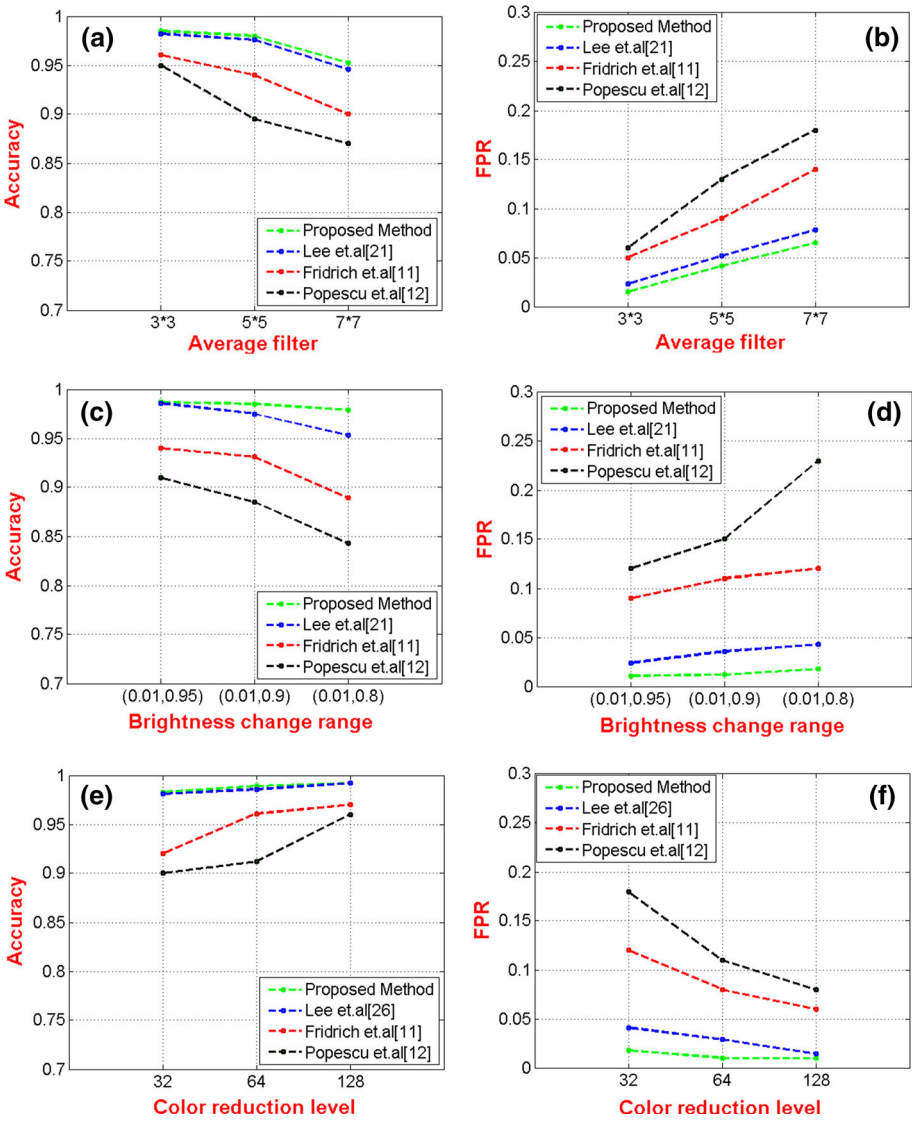

Fig. 12 AR/FPR curves acquired using different methods: **a**, **b** Blurring with different averaging filters, **c**, **d** different brightness change ranges, **e**, **f** different color reduction levels

automatically detects the tampered region with some geometric transformations can be developed in future.

Acknowledgements Authors are thankful to the University Grants Commission (UGC) for the support of Innovative project scheme.

References

1. Mahdian, B., & Saic, S. (2010). A bibliography on blind methods for identifying image forgery. *Signal Processing and Image Communication, 25*(6), 389–399.
2. Satheeshkumar, J., & Thirunavukkarasu, V. (2014). Passive tamper detection techniques in digital images-A survey. NCDS, pp. 237–244.
3. Thirunavukkarsu, V., & Satheesh Kumar, J. (2014). Analysis of digital image forgery detection techniques. *International Conference on Convergence Technology, 4*(1), 1000–1002.
4. Thirunavukkarsu, V., & Satheesh Kumar, J. (2014). Intrusive and non-intrusive techniques for detecting fake images. *IJBI, 3*(1), 374–379.
5. Farid, H. (2009). A survey of image forgery detection. *IEEE Signal Processing, 2*(26), 6–25.
6. Thirunavukkarsu, V., & Satheesh Kumar, J. (2014). Analysis of various noise models and filtering techniques used for image restoration. *IJRCSIT, 3*(1), 4–9.
7. Satheesh Kumar, J., & Thirunavukkarsu, V. (2015). Image splicing detection based on camera characteristics and lighting inconsistencies. *ICIoTC, 1*(1), 10–14.
8. Al-Qershi, O. M., & Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic Science International, 231,* 284–295.
9. Thirunavukkarsu, V., & Satheesh Kumar, J. (2014). Evolution of blind methods for image tamper detection-A review. *IJAER, 9*(21), 5069–5076.
10. Thirunavukkarsu, V., & Satheesh Kumar, J. (2016). A novel method to detect copy-move tampering in digital images. *IND-JST, 9*(8), 1–4.
11. Fridrich, A. J., Soukalm, B. D., Lukas, A, J. (2003). Detection of copy-move forgery in digital images. *Proceedings of Digital Forensic Research Workshop*, pp. 19–23.
12. Popescu, A. C., & Farid, H. (2005). Exposing digital forgeries in color fil-ter array interpolated images. *IEEE Transactions on Signal Processing, 53*(10), 3948–3959.
13. Mehdi G., Mohammad F., Ahmad F. (2011). DWT-DCT (QCD) based copy-move image forgery detection. *IWSSIP*, 1–4.
14. Zhao, J., & Guo, J. (2013). Passive forgeries for copy-move image forgery using a method based on DCT and SVD. *Forensic Science International, 233*(1), 158–166.
15. Bravo-Solorio, S. Nandi, A. K., (2009). Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling. *EUSIPCO*, pp. 824–828.
16. Cao, Y., Gao, T., Fan, L., & Yang, Q. (2012). A robust detection algorithm for copy-move forgery in digital images. *Forensic Science International, 214*(1), 33–43.
17. Chang, C., Cloud, Y., & Chang, C.-C. (2013). A forgery detection algorithm for exemplar-based inpainting images using multi-region relation. *Image and Vision Computing, 31*(1), 57–71.
18. Li, L., Li, S., Zhu, H., & Xiaoyue, W. (2014). Detecting copy-move forgery under affine transforms for image forensics. *Computers & Electrical Engineering, 40*(6), 1951–1962.
19. Guohui L., Qiong W., Dan T., Shaojie S., (2007). A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on dwt and svd. *IEEE International conference on multimedia and expo*, pp. 1750–1753.
20. Yang, B., Sun, X., Chen, X., Zhang, J., & Li, X. (2013). An efficient forensic method for copy–move forgery detection based on DWT-FWHT. *Radio Engineering, 22*(4), 1098–1105.
21. Lee, J.-C. (2015). Copy-move image forgery detection based on Gabor magnitude. *Journal of visual communication image representation, 31,* 320–334.
22. Bashar, M., Noda, K., Ohnishi, N., & Mori, K. (2010). Exploring duplicated regions in natural images. *IEEE Transactions on Image Processing, 9*(9), 1–40.
23. Burges, C. J. C. (2009). Dimension reduction: A guided tour. *Foundations and TrendsR in Machine Learning, 2*(4), 275–365.
24. Kodak Lossless True Color Image Suite [Internet]. [Cited 2016 Apr 27]. http://r0k.us/graphics/kodak.
25. Tralic, D., Zupancic, I., Grgic, S., Grgic, M., (2013). CoMoFoD—New database for copy-move forgery detection. *In Proceedings of 55th International Smposium ELMAR*, pp. 49–54.
26. Lee, J.-C., Chang, C.-P., & Chen, W.-K. (2015). Detection of copy–move image forgery using histogram of orientated gradients. *Information Sciences, 321,* 250–262.
27. Surya Prabha, D., & Satheesh Kumar, J. (2015). Assessment of banana fruit maturity by image processing technique. *Journal of Food Science and Technology, 52*(3), 1316–1327.

V. Thirunavukkarasu received his bachelor degree in Mathematics during 2001 and Master Degree in Computer Applications from STC college, Pollachi during 2004. He has successfully completed Master of Philology in Computer Science during 2006 from Bharathidasan University. He is currently pursuing Ph.D in Computer Science in the Department of Computer Applications, School of Computer Science and Engineering, Bharathiar University, Coimbatore, Tamil Nadu, India. His area of interest include Image processing and its applications on crime domain.

J. Satheesh Kumar is with the Department of Computer Applications, School of Computer Science and Engineering, Bharathiar University, Coimbatore, Tamil Nadu, India. He received his Masters in Computer Applications (MCA) during 1999 and Doctor of Philosophy from scsvm University during 2010. He is having 16 plus years of research and teaching experience. His area of specialization includes soft computing, networks, Image processing and medical imaging.

Gyoo Soo Chae received the B.S. and M.S. degrees in electronic engineering from Kyungpook National University in 1993 and 1995, respectively and Ph.D. degree in electrical engineering from Vitginia Polytechnic Institute and State University in 2000. From January 2001 to February 2003, he was an RF manager at Amphenol Mobile. He is currently a professor of Division of Information & Communication Eng. at Baekseok University since 2003. His current research interests include microwave antenna, EMI(electromagnetic interference) and RF circuits.

J. Kishorkumar is with the Department of Physics, Arignar Anna Government Arts College, Tamil Nadu, India. He received his Masters in Physics during 1994 and Doctor of Philosophy from Bharathiar University during 2014. He is having 20 plus years of research and teaching experience. His area of specialization includes Embedded System, Crystal growth and Electronics.