IJCTA, 9(10), 2016, pp. 4705-4714

Passive Image Tamper Detection Technique Based on Moment Invariants

***V. Thirunavukkarasu **J. Satheesh kumar**

Abstract : The evolution of high-resolution digital cameras, personal computers and dominant image editing tools makes extremely simple to tamper the digital images for malicious purpose. Ensuring authenticity of digital image without the knowledge of image contents is a primary objective of passive tamper detection. This article proposes an efficient and novel passive technique that uses Hu moments to detect and locate the most common type of tampering called copy-move. Experimental results demonstrate that the proposed method effectively discovers simple and multiple copy-move regions, even the tampered region is rotated, blurred and brightness adjusted.
Keywords : Tampering, Hu, Copy-move, blur, malicious.

1. INTRODUCTION

Digital images lost its integrity several years ago due to the rapid growth of inexpensive and easy to use image editing software's. Digital images are tampered for various reasons some tampering is performed with a specific intention (malicious) such as deceiving a court or public others are very kind for example if it is performed for an entertainment or marketing a product (non-malicious)[1][2]. Ensuring trustworthiness of digital images is essential when it is used as an evidence or official document. There exist different ways to produce false proof of an image. Copy-move, image splicing, and retouching are most commonly used methods to tamper the content of an image [3]. In copy-move a specific region of an image is copied and pasted in different part of same image to conceal or duplicate a specific part of an image. Figure. 1 is an example for copy-move image tampering. Image splicing or compositing is simple and most frequently used technique in which two or more image fragments are combined

Fig. 1. (*a*) Original image **(*b*) Copy-move tampered image**

* Department of Computer Applications, School of Computer Science and Engineering, Bharathiar University, Coimbatore (Email: arasu_mca3@yahoo.com) (9487221719),

** Department of Computer Applications, School of Computer Science and Engineering, Bharathiar University, Coimbatore (Email: jsathee@rediffmail.com) (9443968110)

together to make a composite image. Image re-touching is less harmful kind of tampering in which specific features of an image increased or decreased to make the image looking better [4]. Developing a technique that automatically detect and locate the tamper region without depending on pre-embedded code or signature is one of the emerging area of research in image processing[5][6]. Current tamper detection techniques are classified as active and passive. Most active techniques employ digital watermark or digital signature to assess the trustworthiness of an image by embedding authentication code during or after the image acquisition process. However, passive technique does not use pre-embedded authentication code rather it employs user specific algorithm to discriminate tampered version from the original image [7]. Digital image tamper detection has higher influence in most of the application areas such as criminal investigation, law enforcement, journalistic photography, medical imaging and insurance claim processing [8].

Organization of this paper includes section II which reveals some of the related works on copy-move tamper detection. Section III illustrates Hu moment invariants. Proposed methodology is introduced in section IV. Experimental results are discussed in section V. Section VI concludes the paper.

2. RELEATED WORKS ON COPY-MOVE TAMPERING

Many passive tamper detection techniques have been proposed to identify and locate the copy-move image tampering. Farid et al. conducted a detail survey on passive tamper detection techniques and classify it in to five categories such as pixel based, format based, camera based, physically based and geometric based techniques [9]. Zhouchen et al. introduced a method that effectively detects tampered images by examining the double quantization effect concealed along with the discrete cosine transform (DCT) co-efficient. Block posterior probability map (BPPM) is used to differentiate tampered region from the original. This method effectively detects the tamper region even it is post-processed by various methods such as in-painting, texture synthesis and alpha matting [10]. Zimba et al. proposed a method based on Discrete Wavelet Transform (DWT) to decompose the image into four sub bands. Low frequency components are divided into fixed size overlapping blocks to extract the features and radix sort is used to match the image blocks. This method is robust against various post processing operations such as JPEG compression and noise addition but inadequate to handle scaling and rotation [11].

Zhao et al. discovered a method based on Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) to represent fixed size image blocks. This technique decrease the computational complexity by reducing feature dimension and effectively detects copy-move region even it is distorted by Additive White Gaussian Noise (AWGN), JPEG compression and their mixture operation. Accuracy of the method is dropped when Signal Noise Ratio (SNR) is more than 45 db and JPEG quality factor is below 70% [12]. Liu et al. used Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD) to detect and locate the copy-move tampered region. Single level DWT is applied to the suspected image and approximate coefficients are extracted then divided in to overlapping blocks. SVD is applied to each overlapping block and dominant features are selected and matched based on threshold value. This approach effectively detects multiple-copy move forgery even the tampered region is distorted by Gaussian blurring, JPEG compression and their mixed operation [13]. Muhammad et al. developed a method based on un decimated wavelets transform (UWT) and Zernike moments (ZM) to detect copy-move tampering, first the approximate co-efficient of UWT is divided into fixed size blocks then Zernike moment features are extracted from each block, finally Euclidean distance between the pair of blocks are calculated to match the extracted features. This technique effectively detects the tampered region with some geometric transformation, however it fails to detect the tampered region which is blurred or noise contaminated [14]. Liu et al. employs Gaussian pyramid decomposition and circle block method to detect region duplication forgery. This method effectively detects the copy-move region even it is distorted by noise, blurring, JPEG compression and rotation. However feature vectors are extracted only on the inscribed circle of square, pixels outside the inscribed circle area is not processed which leads some false matches [15]. Ryu et al. deployed Zernike moments to fixed sixe image blocks for detecting and localizing the tampered region. Zernike moment feature are invariant against rotation hence, this method effectively detect the tampered region which is rotated under different angles moreover the method effectively detect the tampered region contaminated by Additive White Gaussian Noise (AWGN), JPEG compression and blurring nevertheless, it is not appropriate for tampered region which is scaled or affine transformed [16]. Seung et al. proposed a passive forensics technique to detect and locate the duplicate image region based on Zernike moments. First, Zernike moment features are extracted from the fixed size image blocks up to an appropriate order then locality sensitive hashing (LSH) is deployed to match the block features finally, phase of Zernike moments are calculated to reduce the false matches. This technique exhibits robustness against blurring, JPEG compression, additive white Gaussian noise, and moderate scaling. Zernike moment features are inappropriate to localize a tampered region which is distorted by strong affine transformations other than rotation [17]. Yan et al. developed a method based on Self-adaptive Scale Invariant Feature and Zernike moments. In this method SIFT key points are extracted from the input image using self adaptive threshold method then Euclidean distance between the feature descriptors are calculated to match the SIFT features finally, Zernike moment based region growing process is adopted to every matched pair of feature descriptors to locate the tampered region [18].

3. HU INVARIANT MOMENTS

Moments are scalar quantities used to characterize patterns in an image and extract its important features. Image moments are extensively used in image registration, image reconstruction, computer vision, pattern recognition and its related fields. Geometric, Hu and Zernike are the well- known moments used in variety of pattern recognition applications [19] [20]. Moment features are invariant against translation, rotation and scaling, which facilitates to classify objects on large scale maps. Hu introduced six orthogonal and one skew orthogonal moment feature based on algebraic invariants [21].

The moment for 2D continuous function $f(x,y)$ of order $(r + s)$ is defined as

$$m_{rs} = \iint_{-\infty}^{\infty} x^r y^s f(x, y) dxdy \qquad (1)$$

Where $r, s = 0,1,2.....$

Adapting the equation 1 for 2D gray scale image the raw moment m_{rs} is calculated using the formula

$$m_{rs} = \sum_{x=0}^{p-1} \sum_{y=0}^{q-1} x^r y^s f(x, y) \qquad (2)$$

Where, p and q denotes number of rows and columns in an image.

Zero-order moment (m_{00}) denotes the mass of an image which is obtained with the formula

$$m_{00} = \iint_{-\infty}^{\infty} f(x, y) dxdy \qquad (3)$$

The first order moment m_{10} and m_{01} are commonly used to describe centroid of an image. Moment in equation 1 is not invariant when $f(x, y)$ is changed by translation, rotation or scaling. Invariant features are obtained by central moments which is achieved using the formula

$$m_{rs} = \iint_{-\infty}^{\infty} (x - x')^r \ (y - y')^s \ f(x, y) \ dxdy \qquad (4)$$

Where $r, s = 0,1,2.....$

The centroid x' and y' is defined as follows

$$x' = \frac{m_{10}}{m_{00}} \ y' = \frac{m_{01}}{m_{00}} \qquad (5)$$

Moments obtained using the equation 4 is called centralized moment which is invariant against translation, rotation and scaling. The normalized central moments are defined as follows

$$\lambda_{rs} = \frac{m_{rs}}{m_{00}^{\sigma}} \qquad (6)$$

Where $\sigma = (r + s + 2)/2,\ r + s = 2,3,\ldots.$

Based on normalized second and third order central moments, Hu introduced seven moment features which is invariant under image translation, rotation and scaling [22]. Seven Hu moments are defined as follows

$$M1 = (\lambda_{20} + \lambda_{02}) \quad (7)$$

$$M2 = (\lambda_{20} + \lambda_{02})^2 + 4\lambda_{11}^2 \quad (8)$$

$$M3 = (\lambda_{30} - 3\lambda_{12})^2 + (3\lambda_{21} - \lambda_{03})^2 \quad (9)$$

$$M4 = (\lambda_{30} + \lambda_{12})^2 + (\lambda_{21} + \lambda_{03})^2 \quad (10)$$

$$M5 = (\lambda_{30} - 3\lambda_{12}) + (\lambda_{30} + \lambda_{12}) [(\lambda_{30} + \lambda_{12})^2 - 3 (\lambda_{21} + \lambda_{03})^2] + (3\lambda_{21} - \lambda_{03}) + (\lambda_{21} + \lambda_{03})[(3\lambda_{30} + \lambda_{12})^2 - (\lambda_{21} + \lambda_{03})^2] \quad (11)$$

$$M6 = (\lambda_{20} - \lambda_{02})[(\lambda_{30} + \lambda_{12})^2 - (\lambda_{21} + \lambda_{03})^2] + 4\lambda_{11}(\lambda_{30} + \lambda_{12})(\lambda_{21} + \lambda_{03} \quad (12)$$

$$M7 = (3\lambda_{21} - \lambda_{03}) + (\lambda_{30} + \lambda_{12}) [(\lambda_{30} + \lambda_{12})^2 - 3 (\lambda_{21} + \lambda_{03})^2] + (3\lambda_{12} - \lambda_{03}) + (\lambda_{21} + \lambda_{03}) [(3\lambda_{30} + \lambda_{12})^2 - (\lambda_{21} + \lambda_{03})^2] \quad (13)$$

From the above equations moments M1to M6 are absolute orthogonal invariants which are independent of position, size and orientation and seventh moment M7 is skew orthogonal which is useful in distinguishing mirror images. Seven Hu features (M1, M2, ….M7) are able to recognize simple object even the size, position and orientations are different.

4. PROPOSED TAMPER DETECTIONMETHOD

The most significant function of any tamper detection algorithm is to detect and locate the tampered region under different image distortions such as rotation, scaling, blurring, brightness or color changes. Proposed copy-move tamper detection (CMTD) algorithm consists of four stages such as preprocessing, feature extraction, feature matching and tamper detection. Overall framework of proposed CMTD method is shown in figure 2.

4.1. Image Preprocessing

In the first stage the suspected input image is converted into gray scale using the standard gray scale conversion formula,

$$Y = 0.299\ R + 0.587\ G + 0.114\ B \quad (14)$$

Where, R, G, and B are the three color channels of suspected image and Y represent its luminance component.

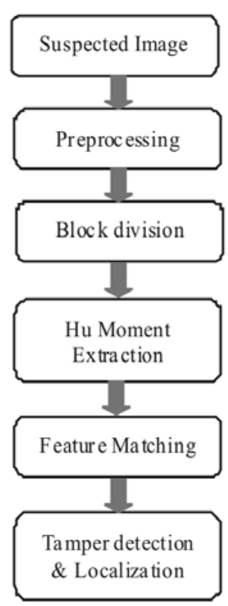


Fig. 2. Frame work of proposed tamper detection method

4.2. Feature Extraction

The preprocessed input image is divided into fixed size overlapping blocks of size b X b, by sliding one pixel from upper left corner to lower right corner. Total number of overlapping blocks should not exceed (M-b+1)(N-b+1) where, M and N are total number of rows and columns in the input image. Size of the blocks must be smaller than the size of tampered region. Here size of overlapping block is set to 8 X 8. After block division the seven Hu moments from each overlapping blocks are extracted as a feature vector. Dimension of feature vector are compared with existing methods DCT & SVD [12] and Zernike method [14] whose feature dimension is 1 X 16 and 1 X 36 respectively. However, the proposed method reduces the feature dimension as 1X 7.

4.3. Feature Matching

The Extracted features are stored in two dimensional matrix F with size (M – b + 1)(N – b + 1) X 7.

$$F = \begin{bmatrix} f_1 \\ f_2 \\ \cdot\cdot \\ \cdot\cdot \\ f_{(M-b+1)(N-b+1)} \end{bmatrix}$$

If the two rows of feature matrix F is similar enough their corresponding block are similar. Matching similar blocks in the image is performed by lexicographically sorting each row in a matrix F and makes the similar blocks adjacent to each other.

4.4. Tamper detection and localization

Each row of a two dimensional matrix F is compared with all other rows to identify similar block pair. If two rows are similar enough the algorithm finds the sift vector S between similar rows to remove the false matches. If the sift vector occurrence exceeds the user specified threshold T subsequently position of block pairs are stored in a separate matrix to locate the tampered region. Sift vector S is calculated using the formula,

$$S = \|x_1 - y_1, x_2 - y_2\| \tag{15}$$

Where x_1, x_2 and y_1, y_2 are the position of matching block pair.

5. EXPERIMENTAL RESULTS

To evaluate the performance and robustness of proposed copy-move tamper detection method a series of experiments were carried out with two different data sets. The first data set CoMoFoD consists of 200 color images of size 512 X 512 released by video communication laboratory. Within this data set the copied regions are from different categories of natural, living, and mixed images. Tampering is performed by copying, scaling and rotating meaningful image regions. Moreover JPEG compression and noise addition is made to the tampered images [23]. Kodak image data set is second data set which contain 24 un- compressed true color images of size 768 X 512 released by Kodak corporation for unrestricted research purpose [24]..

5.1. Performance Evaluation

To demonstrate the performance of proposed method two evaluation criteria such as correct detection rate (CDR) and False Detection Rate (FDR) were used. It is defines as follows,

$$CDR = \frac{|\cap^{TT}| + |\mu \cap \mu \quad|}{|| + |\mu|} \tag{16}$$

Where CDR indicates the performance of proposed algorithm correctly locating the pixels of tampered region, and μ indicates the pixels of original and tampered region in original image. T and μ^T specifies the pixels of original and tampered region in the detected result image, $\cap$ indicates the intersection of two regions.

$$\text{FDR} = \frac{|^{TT}-| + |\mu \quad -\mu|}{|^{T}| + |\mu^{T}|} \tag{17}$$

Where, FDR reveals the amount of pixels which are not contained in duplicated region but wrongly incorporated by the proposed method, – indicates the difference of two regions. The proposed method effectively detect simple and multiple copy-move region even the tampered region is too small. Figure 3 shows the detection result of simple and multiple tampered regions.

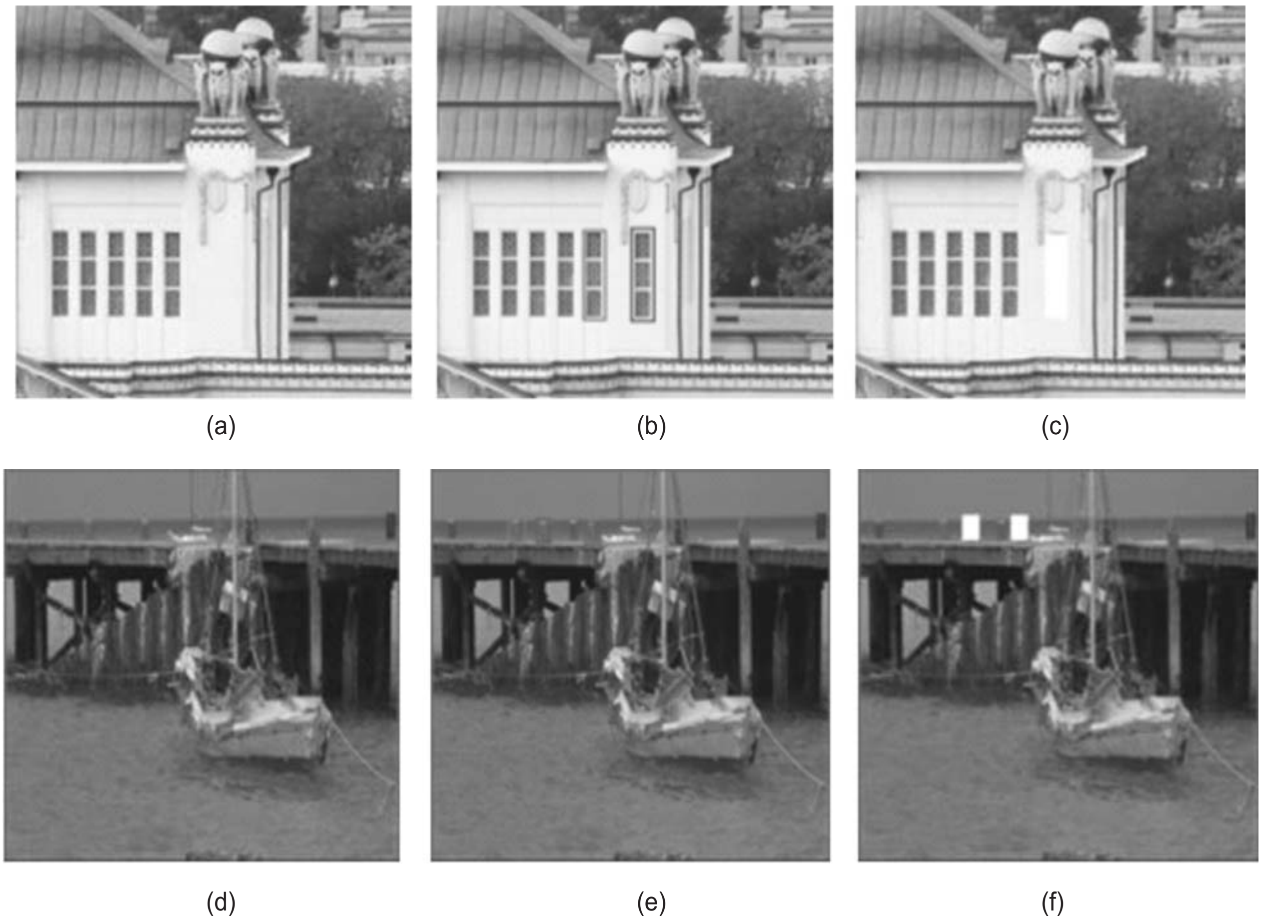
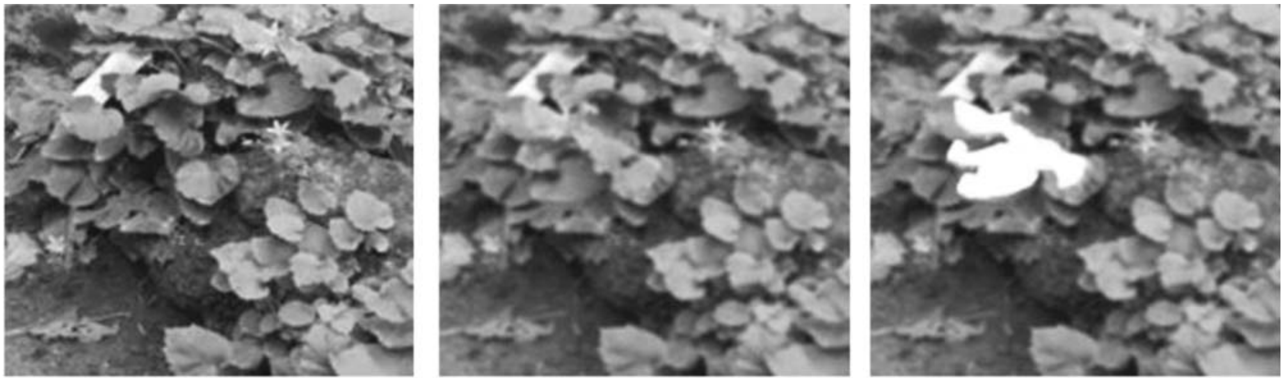


Fig. 3. **(*a*) and (*d*) Original images, (*b*) and (*e*) Simple and multiple copy-move tampered images, (*c*) Detection result of (*b*), (*f*) Detection result of (*e*).**

5.2 Robustness test

5.2.1 Analysis of robustness against blurring and brightness change

In addition to simple and multiple copy-move tamper detection, the proposed method is also tested With tampered image which is distorted by blurring and brightness change. Three different averaging filters with 3 X 3, 5 X 5 and 7 X 7 averaging masks are used to blur the tampered image. The proposed method obviously exhibit high detection performance when the tampered images are distorted with 3 X 3 and 5 X 5 averaging filters. Figure 4 (b) and (c) are tampered image blurred with 7 X 7 averaging filter and its corresponding detection result. Performance of proposed method is also tested with the effects of changes in brightness. Brightness of the image is changed by mapping the original image intensity values between lower and upper bounds at the intervals [0,1]. This resulted in images in three ranges of brightness ([0.01, 0.95], [0.01, 0.9] and [0.01, 0.8]). Tampered image with brightness change in the range [0.01, 0.9] and its detection result is shown in figure 4 (e) and (f) respectively. Table 1 illustrate the detection performance of proposed method.



(a) (b) (c)

(d) (e) (f)

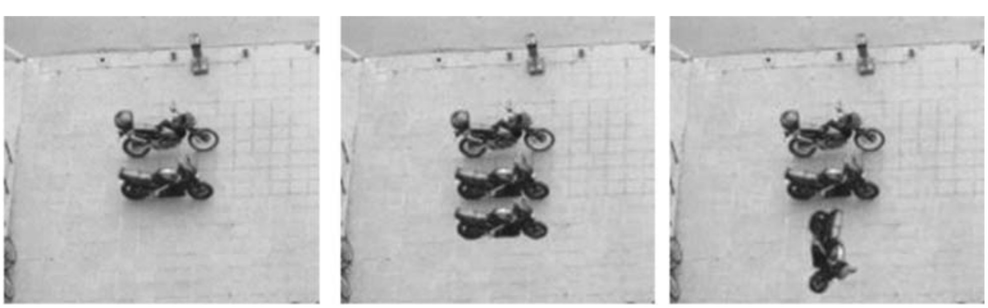
Fig. 4 (*a*) and (*d*) Original images, (*b*) Tampered image blurred with 7 X 7 averaging filter, (*c*) Detection result of (*b*), (*e*) Tampered image with brightness altered [0.01, 0.9], (*f*) Detection result of (*e*)

Table 1. Detection performance of proposed method

Image	*Type of tampering*	*Performance of proposed method*	
		CDR	*FDR*
Figure 3(c)	Simple	0.995	0.001
Figure 3(f)	Multiple	0.995	0.003
Figure 4(c)	Blurring	0.977	0.004
Figure 4(f)	Brightness change	0.984	0.012

5.2.2 Analysis of robustness against rotation

Rotation is most common type of geometric transformation used to hide the traces of image tampering. In this method the tampered region copied, Rotated and translated in to different part of the same image [23]. Proposed method exhibit good performance even the tampered region is rotated with different angles. Figure 5 shows the detection result of tampered images with different degree of rotation. Figure 5(*c*), (*d*) and (*e*) are tampered image region rotated with clockwise 90 degrees, counter clockwise 90 degrees and 180 degrees respectively. Figure 5 (*f*), (*g*) and (*h*) are corresponding detection results.



(a) (b) (c)

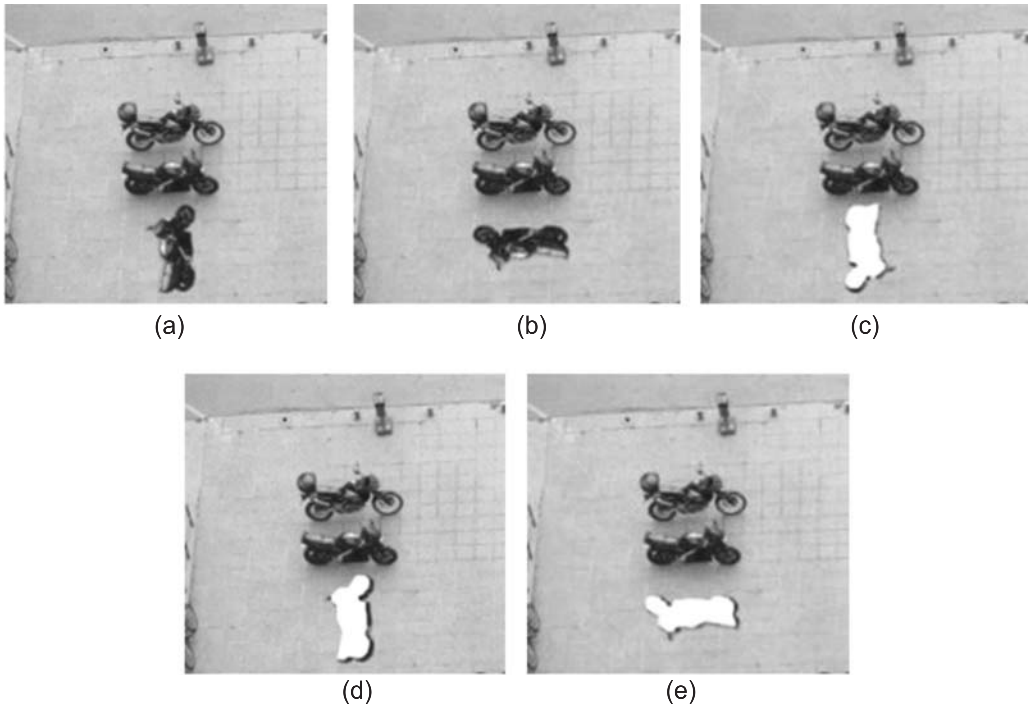


Fig. 5. Examples of copy-move tampering with typical geometric transformation and its corresponding detection result.

5.3. Comparison with existing approaches

Experimental results demonstrate that the proposed method effectively detect simple, multiple copy-move forgery under various image distortions and the result are compared with existing method in-terms of computational complexity and accuracy. Computational complexity is an important problem in any tamper detection technique, dimensionality of a feature vector place a vital role to reduce the computation complexity. Total number of rows in a matrix F in section 4.3 indicates number of blocks and total number of columns indicates the feature dimension. Table 2 shows the comparison of feature dimension with existing methods.

Table 2. Comparison of feature dimension

Method	*Algorithm*	*Feature Dimension*
Zhao et.al [12]	DCT & SVD	16
Mohammed et.al [14]	UDWT & Zernike Moments	36
Proposed	Hu Moments	7

5.3.1. Accuracy comparison

In this section accuracy of proposed method is compared with existing methods in terms of Correct Detection Rate (CDR) and False Detection Rate (FDR). Kodak image data set images with resolution 768 X 512 used by DCT and SVD method [12] are tested by the proposed method and the appropriate detection results are displayed in figure 6 (c) and (f) respectively. CDR and FDR values of DCT and SVD method and proposed method are listed in Table 3. Experimental results in Table 3 indicates, the correct detection rate of the proposed method is greater than 0.96 and False Detection Rate is close to 0, which shows the proposed method perform better to detect the tampered region more accurately then the existing method. Overall CDR and FDR values of proposed method indicate the better detection performance even the tampered region is too small and distorted by different post-processing operations such as rotation, blurring and brightness change.

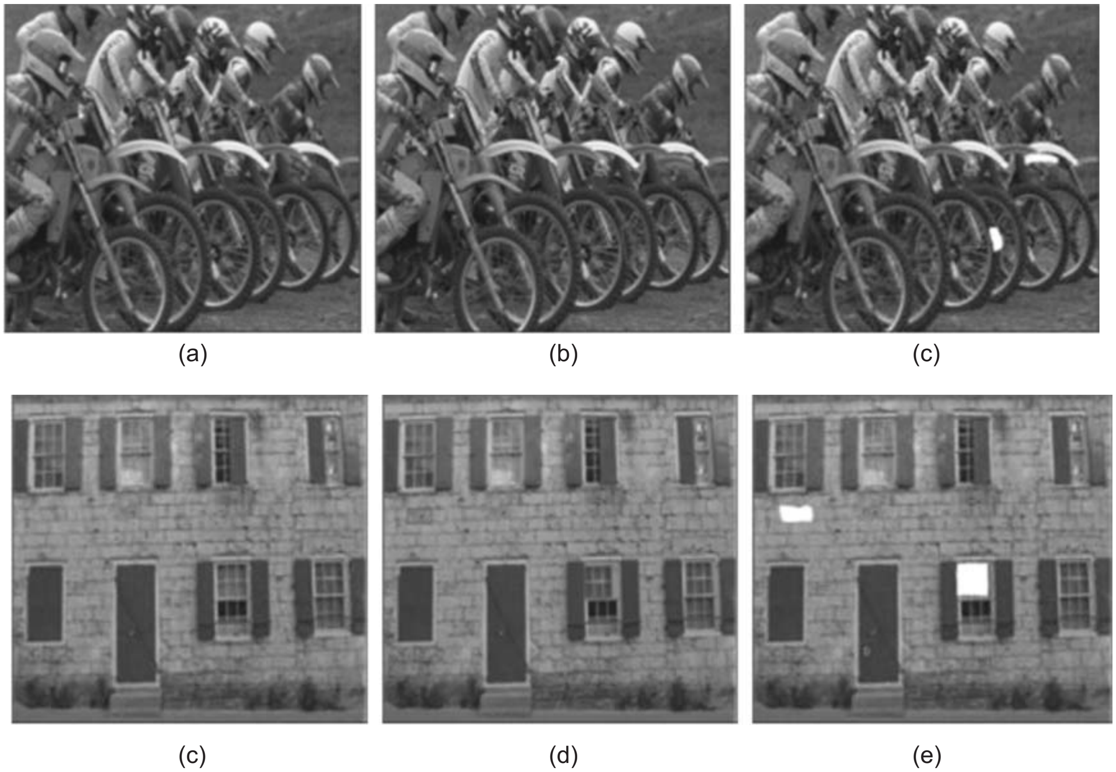


Fig. 6. (*a*) and (*d*) original images, (*b*) Multiple non-regular forged image, (*c*) Detection result of (*b*), (*e*) Multiple forged image with Gaussian blurring, (*f*) detection result of (*e*).

Table 3. Detection accuracy of DCT and SVD method and proposed method

Image	*Type of Tampering*	*DCT and SVD Method [12]*		*Proposed*	
		CDR	*FDR*	*CDR*	*FDR*
Figure 6(*c*)	Multiple	0.929	0.003	0.995	0.002
Figure 6(*f*)	Blurring with std 1.0	0.938	0.008	0.991	0.004
Figure 6(*f*)	Blurring with std 3.0	0.912	0.011	0.963	0.002

6. CONCLUSION

In this article an efficient passive copy-move tamper detection technique based on Hu moment invariants are proposed. The proposed method performs extremely well to detect simple and multiple copy-move regions without depending on watermark or digital signature. Experimental results demonstrate that the proposed method effectively detect and locate tampered region even it is rotated, blurred, brightness adjusted. Comparing to the existing method the proposed method has higher accuracy and lower computational complexity.

7. REFERENCES

1. Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, Elli Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Transactions on Information Forensics and Security, Vol. 7(6), 2012, pp:1-26.
2. Osamah M, Al-Qershi , Bee Ee Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art", Forensic Science International, Elsevier publication (2013), pp:284–295.
3. V.Thirunavukkarsu, J.Satheesh Kumar, "Analysis of Digital Image Forgery Detection Techniques", International Conference on Convergence Technology (ICCT), Vol. 4(1), 2014, korea convergence society, pp:1000-1002.
4. V.Thirunavukkarasu , J.Satheesh Kumar , "Intrusive and non-intrusive techniques for detecting fake images", Inter-national Journal of Business Intelligence, Vol. 3(01), 2014, pp: 374– 379.

5. Gajanan K Birajdar, Vijay H Mankar, "Digital image forgery detection using passive techniques: A survey", Digital Investigation, Vol. 10(3), 2013, pp: 226–245.

6. Babak Mahdian, Stanislav Saic, "A bibliography on blind methods for identifying image forgery", Signal Processing and Image Communication, vol. 25(6), 2010, pp: 389–399.

7. V.Thirunavukkarasu, J.Satheesh Kumar, "A Novel Method to Detect Copy-Move Tampering in Digital Images", Indian Journal of Science and Technology (IND-JST), Vol. 9(8), 2016.

8. V.Thirunavukkarasu, J.Satheesh Kumar , "Evolution of Blind Methods for Image Tamper Detection-A Review", International Journal of Applied Engineering Research (IJAER) ,vol. 9(21), 2014, pp:5069-5076.

9. Farid H, "A survey of image forgery detection", IEEE Signal Processing, Vol. 2(26), 2009, pp: 6–25.

10. Zhouchen Lina, JunfengHeb, XiaoouTanga, Chi-KeungTang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis", Pattern Recognition , Vol. 42, 2009, pp: 2492 – 2501.

11. Michael Zimba, Sun Xingming, "Fast and Robust Image Cloning Detection using Block Characteristics of DWT Coefficients", International Journal of Digital Content Technology and its Applications, Vol. 5(7), 2011, pp:359-367.

12. Jie Zhao, Jichang Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD", Forensic Science International, Vol. 233(1), 2013, pp: 158–166.

13. Feng Liu, Hao Feng, "An efficient algorithm for image copy-move forgery detection based on DWT and SVD", International Journal of Security and Its Applications Vol.8(5), 2014, pp:377-390.

14. Ghulam Muhammad, Muhammad Hussain, "Passive Detection of Copy-Move Image Forgery using Undecimated Wavelets and Zernike Moments", International Journal on Information, Vol.16(5), pp:2957-2964.

15. Guangjie Liu, JunwenWang, ShiguoLian, ZhiquanWang, "A passive image authentication scheme for detecting region-duplication forgery with rotation", Journal of Network and Computer Applications, 2011, Elsevier publications, pp: 1557–1565.

16. Ryu, Seung-Jin, Min-Jeong Lee, Heung-Kyu Lee, "Detection of copy-rotate-move forgery using zernike moments", Information Hiding, Springer Berlin Heidelberg, 2010.

17. Seung-Jin Ryu, Matthias Kirchner, Min-Jeong Lee, Heung-Kyu Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments", IEEE Transactions on Information Forensics and Security, vol. 8(8), August 2013, pp:1355-1369.

18. Wo YAN, Ruotao XU, Peinan LUO, Xuhui YANG, Hengrui QIN, "A SIFT and Zernike Moment Based Copy-move Forgery Detection Algorithm", Journal of Computational Information Systems, August 2015, pp: 5661-5671.

19. H.Ming-Kuei, "Visual pattern recognition by moment invariants", Information Theory, IRE Transactions, vol. 8, pp.179-187, 1962.

20. M. R. Teaque, "Image Analysis via the General Theory of Moments", Journal of the Optical Society of America, vol. 7, pp. 920-930.

21. Seung-Jin Ryu, Matthias Kirchner, Min-Jeong Lee, and Heung-Kyu Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments", IEEE Transactions on Information Forensics and Security, Vol. 8(8), 2013, pp: 1355-1370.

22. Guangjie Liu, JunwenWang, ShiguoLianb, ZhiquanWang, "A passive image authentication scheme for detecting region-duplication forgery with rotation", Journal of Network and Computer Applications, Elsevier publication (2011), pp: 1557–1565.

23. Tralic D, Zupancic I, Grgic S, Grgic M, "CoMoFoD - New Database for Copy-Move Forgery Detection", in Proc. 55th International Smposium ELMAR-2013, PP: 49-54.

24. Kodak Lossless True Color Image Suite [Internet]. [Cited 2016 Mar 27]. Available from: http://r0k.us/graphics/kodak