I.J. Image, Graphics and Signal Processing, **2015, 6, 38-44**
Published Online May 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2015.06.05

Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors

Sunil Kumar and J. V. Desai
Mody University of Science and Technology, Lakshmangarh, 332311, India
Email: skvasistha@ieee.org

Shaktidev Mukherjee
Moradabad Institute of Technology, Moradabad, India
Email: mukherjee.shaktidev@gmail.com

***Abstract*—**Copy move forgery detection is a very popular research area and a lot of methods have been suggested by researchers. However, every method has its own merits and weaknesses and hence, new techniques are being continuously devised and analyzed. There are many post processing operations used by the manipulators to obstruct the forgery detection techniques. One such operation is changing the contrast of the whole image or copy moved regions, which many existing methods fail to address. A novel method using binary discrete cosine transform vectors is proposed to detect copy move forgery in the presence of contrast changes. The image is divided into overlapping blocks and DCT coefficients are calculated for these blocks. Feature vectors are created from these blocks using signs of the DCT coefficients. Coefficient of correlation is used to match resulting binary vectors. The experiments show that the proposed method is able to detect copy move forgery in presence of contrast changes. The proposed method is also invariant to other post processing operations like Gaussian noise, JPEG compression and little rotation and scaling.

***Index Terms*—**Copy move forgery, intensity invariant forgery detection, binary DCT coefficients, contrast invariant forgery detection, illumination invariant, blind forgery detection

I. INTRODUCTION

Images are a major source of information exchange in the digital world. Digital images are used to illustrate facts, establish facts and used by the newspapers to strengthen the stories published. Also digital images are used as corroborative evidences in criminal investigation. So, it is very much necessary to ensure the truth of what is being believed. The issue of forged images is not new, but with the advancement of technology, it has become easier to manipulate an original image either to mislead the audience or to form a particular public perception about famous personalities. Many instances [1] have been reported in the past to justify the claim. Digital image forgery detection has been growing very fast in the recent years as research domain [2]. Broadly, the forgery techniques can be classified in to Copy move forgery or cloning , splicing and retouching [3] . In splicing, some part of intended image is replaced by the content from some other image as shown in Fig.1. So, the statistical parameters of that region are quite different from rest of the image. Statistical techniques are applied to detect such forgeries. However, in copy move forgery same image content is used to hide some region of the same image as shown in Fig.2.

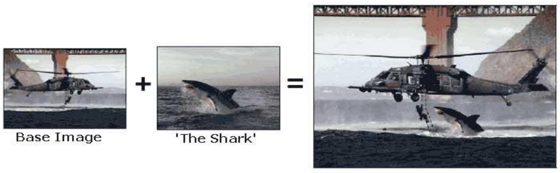


Fig. 1.

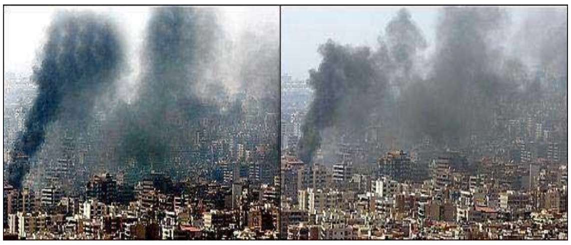


Fig. 2. Forged image on the left and original image on the right

Forgery detection techniques can be classified into two broad categories [4]; active and passive or blind. In active techniques some prior knowledge is used about the original image to detect the tampering in the presented image. One example of such technique is digital watermarking[5]. In passive or blind techniques, there is no prior information available about the original image. Copy move forgery detection using blind methods has picked up as hot research topic due to its wide veracity and applicability. The very fact about natural images, that no significant regions are exactly same in an image is exploited in all such techniques. So, if there is a sizable region to hint duplication then that is treated as case for copy move forgery. Block methods are used to divide the image into overlapping regions and then blocks are compared to find duplication. The different issues in such techniques are the time taken, efficient feature collection from the blocks, and matching techniques to efficiently find similar blocks. Also, to make the detection of forgery difficult, some post copy move operations like adding some noise, compressing the manipulated image etc. are generally applied. One such operation is to make changes in the intensity values of either full presented image or local regions to escape from the detection techniques. In the present paper, such post processing operations are taken into consideration and a method invariant to contrast change is being proposed. Experimental observations suggest that the method successfully detect forgery in the presence of brightness as well as contrast changes. The proposed method is compared with the state of the art methods available for copy move forgery detection.

The remaining paper is organized as follows: section II provides a brief survey of the major contributions from the literature in the domain of copy move forgery detection. Section III contains the concept of binary DCT vectors, matching criteria and the proposed algorithm. Section IV contains the experimental setup, the output of the proposed method on sample images and comparison of the proposed method with existing methods. Section V concludes the work done and scope for future enhancements in the proposed work.

II. Related Work

Most of the methods used for detecting copy move forgery use two approaches. One is the block based approach in which the image in question, is divided into overlapping blocks and these blocks acts as input to transform and matching phase. The other approach, is the key point based approach, where keypoints are detected and descriptors at these keypoints are calculated and matched. The first block based method was proposed by Fridrich et al.[6], based on discrete cosine transform (DCT). Popescu and Farid [7] altered the block representation and instead of DCT used principal component analysis (PCA). Sunil Kumar et al. [8] suggested a method by applying PCA on DCT domain to achieve robustness against both noise and JPEG compression. It also achieves invariance to illumination, but fails to detect contrast variations. Huang et al [9] suggested an improved method using DCT coefficients. Luo et al [10] divided blocks into four sub-blocks, which were evaluated according to an average of red, blue and green color values. This method proved robust to attacks, such as JPEG compression, Gaussian blurring, and additive noise. An approach using combination of DWT and DCT is suggested in [11]. Discrete wavelet transform is used to reduce the size of image and then, DCT is applied on low frequency component achieved by DWT. Singular value decomposition (SVD) is applied to each image block to yield a representation with reduced dimensions in [12]. This approach proved robust against noise distortion and more efficient. DCT blocks are converted into circular blocks and divided into four regions to get feature vectors in [13]. Local binary patterns are used to get the binary feature vector for robust and efficient matching in [14] [15]. Bayram et al. [16] applied a Fourier Mellin transform (FMT) and 1-D projection of log-polar values in a robust scheme for the detection of image forgeries. Lynch et al. [17] proposed an efficient expanding block algorithm based on direct block comparison rather than indirect comparisons based on block features. Local interest points (e.g. SIFT and SURF) have been widely used for image retrieval and object recognition, due to their robustness in dealing with numerous geometrical transformations (such as rotation and scaling) and occlusions. Recently, attempts have been made to apply these types of features in digital forensics. Keypoint based methods differ from block based methods in their reliance on the identification and selection of regions of high entropy within an image (i.e. “key points”). Scale invariant feature transform (SIFT) is used in [18][19], which is capable of detecting and describing clusters of points belonging to cloned areas. Amerini et al. [20] developed a SIFT based method for the detection of copy move attacks and transformation recovery. Another key point based method using speeded up robust features (SURF) is used in [21] which is faster than SIFT. Jaberi et al [22] used SIFT like feature MIFT to claim higher robustness. However, all the keypoint based methods are having limitations of key point extraction, as keypoints from specific locations only can be extracted. Moreover, copied region with little textural structure may be missed entirely. So, both approaches have their strengths and limitations. This paper proposes a block based method which employs binary DCT feature vectors to transform a block of image into a row vector. Rigorous experiments have been conducted to demonstrate the robustness of the proposed method in dealing with intensity variant post processing operations such as contrast change, noise addition and JPEG compression.

III. Method

A. Discrete Cosine Transform

DCT has been widely used to represent the image in frequency domain due to its ability to represent most of the intensity distribution details with fewer coefficients. The proposed forgery detection algorithm is based on DCT. The overlapping blocks of the image are represented by corresponding DCT coefficients as per equation (1). The intensity of image at pixel (x, y) is I(x, y) and the block size is ‘b’.

$$D(u,v) = \frac{2}{b} C(u) C(v) \sum_{x=0}^{b-1} \sum_{y=0}^{b-1} I(x,y) \cos\left(\frac{\pi u(2x+1)}{2b}\right) \cos\left(\frac{\pi v(2y+1)}{2b}\right) \tag{1}$$

where $C(u) = \begin{cases} \frac{1}{\sqrt{2}} & if\ u = 0 \\ 1 & otherwise \end{cases}$ *and C (v)* is similar to *C (u).*

The DCT coefficients have the property of energy localization. The first DCT coefficient represents the average intensity over the block image. It is called DC coefficient. The other coefficients represent the variations in the intensity and are termed as AC coefficients. The

DCT coefficients are arranged in zig-zag order, such that low frequency coefficients precede high frequency coefficients. By normalizing the low frequency DCT coefficients the vector of DCT coefficient can be made intensity invariant [8] , but still they are not contrast invariant.

B. Binarized Discrete Cosine Transform

To make the row vectors contrast invariant we have proposed a binary form of DCT vector. It has been observed that the signs of the DCT coefficients do not change by the change of contrast of image up to certain level. This property has been exploited in the present work to make the forgery detection method invariant to any change in the contrast of copy moved region only or whole image. The row vectors are converted into binary vector by the following formula: if a row vector r_m of 'n' DCT coefficients is represented by (2)

$$r_m = c_{m0}, c_{m1}, c_{m2}, ..., c_{mn} \tag{2}$$

, then DCT coefficient c_{mn} is modified as follows:

$$c'_{mn} = \begin{cases} 1 & \text{if } c_{mn} > 0 \\ 0 & \text{else} \end{cases} \tag{3}$$

After applying this operation the resultant row vectors are simply binary vectors and termed as DCT binary vectors.

C. Feature Vector Matching

For matching the near duplicate regions, corresponding feature vectors must be matched. Three techniques have been tried namely Euclidean distance, Hamming distance and coefficient of correlation. The later has worked best in the proposed method. Coefficient of correlation between two binary vectors in (4) and (5)

$$r_m = c'_{m0}, c'_{m1}, c'_{m2}, ..., c'_{mn} \tag{4}$$

$$r_{m'} = c'_{m'0}, c'_{m'1}, c'_{m'2}, ..., c'_{m'n} \tag{5}$$

, is calculated as follows:

$$\rho(r_m, r_{m'}) = \frac{Cov(r_m, r_{m'})}{\sqrt{Cov(r_m, r_m) Cov(r_{m'}, r_{m'})}} \tag{6}$$

The row vectors beyond a threshold are considered as similar vectors.

D. Algorithm Flow

(1). Any gray scale image I of the size m x n is input image. Color image can be converted to a grayscale image using the standard formula $I = 0.299R + 0.587G + 0.114B$.

(2). A square window of size b x b is slided across the image I to get $(m\text{-}b +1) \times (n\text{-}b +1)$ overlapping blocks.

(3). Apply two dimensional DCT to each block, and reshape to form a row vector using zig-zag order. Size of such row vector is $1 \times b^2$.

(4). Convert the row vectors into binary DCT vectors using (3).

(5). Retain only fraction α coefficients of the binary row vectors to form matrix of size $(m\text{-}b +1) \times (n\text{-}b +1) \times \alpha b^2$.

(6). The resultant matrix is lexicographically sorted to sort the row vectors according to their similarity.

(7). To further remove the outliers, similarity bins are created of size N_n and vectors having correlation coefficient greater than thresh hold ρ_t are retained as duplicate vectors.

(8). If the distance between duplicate vectors (N_d) is greater than block size, then corresponding locations of such vectors in the image I are stored in two matrices B_1 and B_2.

(9). Scalar shifts are calculated as $|B_1\text{-}B_2|$. The frequency of such shifts is calculated and vectors having highest frequency are finally marked as duplicate region in the given image.

(10). Finally, morphological operations are applied to remove the isolated points and show the binary image I' as output image representing copy moves regions with white regions.

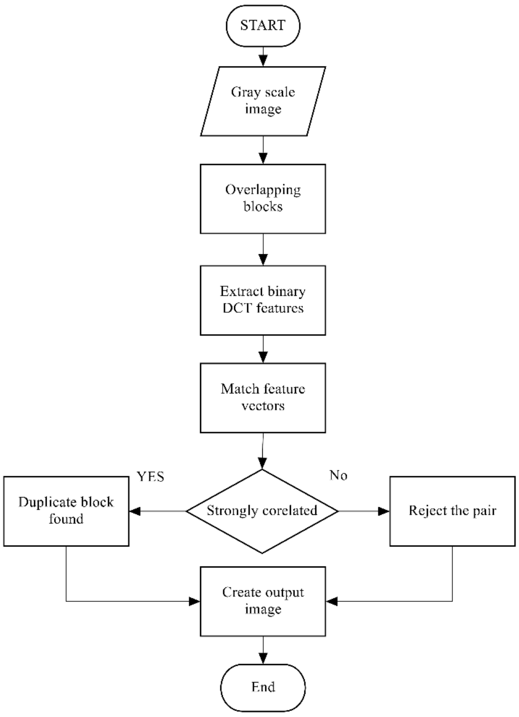


Fig. 3. Algorithm framework

IV. Experimental Results

A. Experimental Setup

The method is tested on two databases[23] and [24]. Also, some images are captured with personal camera. There are total 200 images taken for the experiment in which 20 original images are taken and rest are forged ones with change of contrast in the interval of 15 from -

75 to +75. Also the experiment is divided in two parts .In the first part contrast variation is performed on whole of the image after forgery and in the second part contrast of the forged region is only varied. Any change of contrast beyond the specified range will lead to visible clues of manipulation. Also, the method is tested for robustness against noise, JPEG compression ratio and small rotation and scaling. For testing robustness of the algorithm against added noise, zero mean Gaussian noise is added to the forged images ranging from SNR 90db to 40db. Also, some images are compressed using JPEG compression with compression ratio upto 70%. Block size is taken to be 4 to detect even the small forged regions. The bin size N_n for storing similar vectors is taken 1000. The value of thresh hold ρ_t is taken as 0.9. The feature vector length is restricted by setting α to ¼. The algorithm is coded in MATLAB 2013a on a machine equipped with Intel i5 2.5 GHz processor with 8GB DDR3RAM.

B. *Performance Evaluation Parameters*

The performance of the method is evaluated according to following criteria:

$$D_c = \frac{p(I) \bigcap p(I') + q(I) \cap q(I')}{p(I) + q(I)} \tag{7}$$

$$D_f = \frac{p(I) - p(I') + q(I) - q(I')}{p(I') + q(I')} \tag{8}$$

, where D_c, D_f are the correct detection ratio and false detection ratio respectively. *I* and *I'* are the given image and the output image after applying the forgery detection algorithm. *p(I)* represents the number of pixels covered by the original area in image *I*, *q(I)* represents the number of pixels in the forged region in the given image *I*. Intersection represents the common areas detected correctly. Difference represents the falsely identified pixels either original or forged. So, D_c represents the precision with which the algorithm detects the forged areas. Larger D_c is better. D_f represents imprecision, hence lower is better. D_c, D_f are measure of stability of the method. Also, the ability to detect the forged area correctly is represented by '*e*' i.e. detection efficiency.

$$e = \frac{q(I) \cap q(I')}{q(I)} \tag{9}$$

C. *Performance Analysis*

Following tables are providing the performance analysis of the proposed method with various parameters like local and global change of contrast, addition of Gaussian noise, compressing the forged image and performance comparison with the existing methods.

Table 1. Performance of the algorithm against positive variations of contrast

Performance parameters		Contrast variation range				
		0 ~5	15~ 30	30~45	45~60	60~75
D_c	local	0.9980	0.9982	0.9982	0.9890	0.9911
	global	0.9985	0.9985	0.9985	0.9817	0.9817
D_f	local	0.0019	0.0017	0.0017	0.0109	0.0088
	global	0.0014	0.0014	0.0014	0.0182	0.0182
e	local	0.90	0.90	0.90	0.50	0.51
	global	0.92	0.92	0.92	0.48	0.41

Table 2. Performance of the algorithm against negative variations of contrast

Performance parameters		Contrast variation range				
		-75 ~ -60	-60 ~ -45	-45 ~ -30	-30 ~ -15	-15 ~ 0
D_c	local	0.9887	0.9918	0.9968	0.9963	0.9980
	global	0.9814	0.9817	0.9985	0.9985	0.9985
D_f	local	0.0112	0.0081	0.0031	0.0036	0.0019
	global	0.0187	0.0182	0.0014	0.0014	0.0014
e	local	0.40	0.55	0.84	0.85	0.91
	global	0.52	0.60	0.92	0.92	0.93

Table 3. Performance of the algorithm against JPEG compression ratio in %

Performance parameters	Compression ratio		
	100 ~ 92	91 ~ 85	84 ~ 77
D_c	0.9956	0.9913	0.9874
D_f	0.0106	0.0157	0.0173
e	0.85	0.71	0.40

Table 4. Performance of the algorithm against Gaussian noise in SNR

Performance parameters	Signal to noise ratio				
	90	80	70	60	50
D_c	0.9985	0.9974	0.9964	0.9818	0.9816
D_f	0.0034	0.0056	0.0106	0.0107	0.0181
e	0.92	0.86	0.74	0.62	0.50

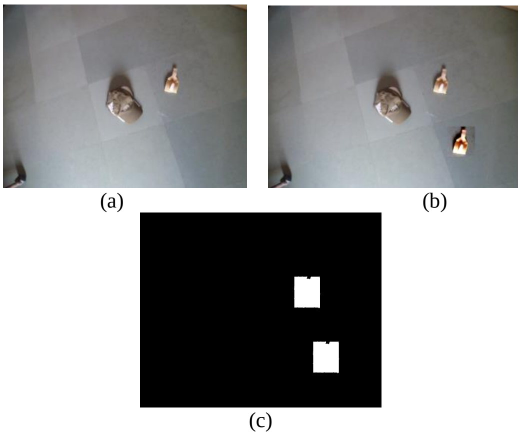
Table 5. Comparison of efficiency of the proposed method with existing methods against variations of contrast

Contrast variation range	Detection efficiency 'e'			
	DCT[6]	PCA[7]	Improved DCT[9]	Proposed method
-25 ~ -20	0.00	0.00	0.00	0.87
-20 ~ -15	0.00	0.00	0.05	0.90
-15 ~ -10	0.12	0.00	0.32	0.92
-10 ~ -5	0.32	0.02	0.41	0.93
-5 ~ 0	0.51	0.21	0.52	0.95
0 ~ +5	0.42	0.22	0.46	0.95
+5 ~ +10	0.32	0.05	0.41	0.94
+10 ~ +15	0.11	0.00	0.21	0.93
+15 ~ +20	0.00	0.00	0.00	0.92
+20 ~ +25	0.00	0.00	0.00	0.90

D. Discussion

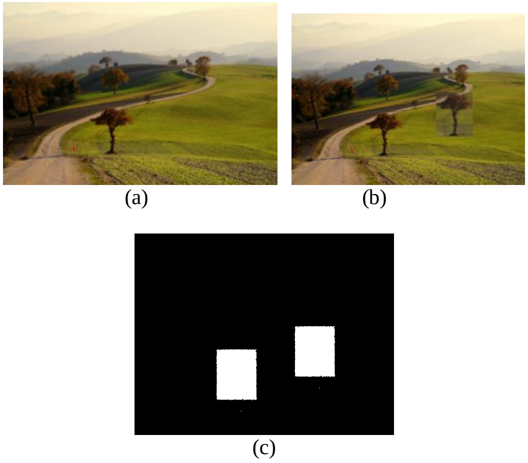
The results in Table 1 and Table 2, show high values of 'D_c' and 'e' , hence, the proposed method is stable and works with good detection efficiency for contrast variations from -45 to +45 on a scale of 100. Subsequently, there is steep fall in the detection efficiency. Although, the detection efficiency dips for large variations of contrast, the stability parameters are good and hence, very low false positives are reported. Also, practically the contrast variations may not go beyond this range. Another observation from the data is that global variations of contrast are easier to tackle than the local ones. Table 3 shows the performance of the method against JPEG compressions and the proposed method detect forgery efficiently up to 80% compression ratio. The method is also quite robust against Gaussian noise addition and works efficiently up to SNR value 60% as shown in Table 4. Comparison with the popular block based methods is given in Table 5. The proposed method outperforms the existing compared methods in terms of the detection area efficiency. Also, the length of the feature vector used in the proposed method is only 4, which is lesser than the compared methods.

E. Visual Results


(a) (b)

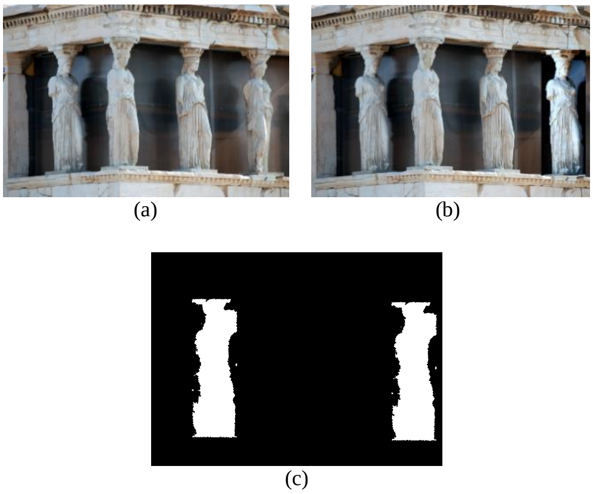
(c)

Fig. 4. Result of forgery detection in the presence of local contrast variation of +20 (a) Original image (b) Forged image (c) Detection result


(a) (b)

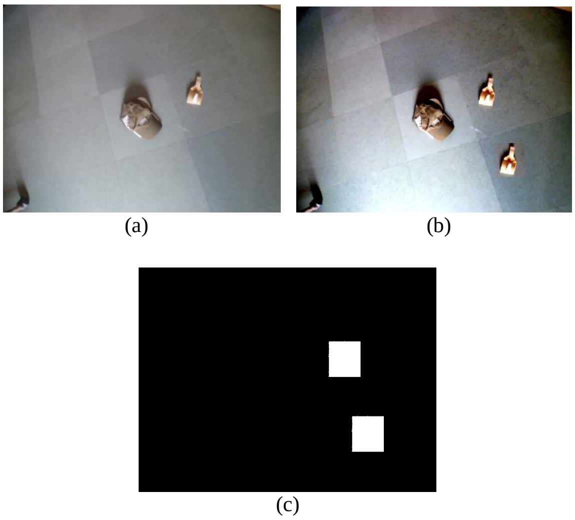
(c)

Fig. 5. Result of forgery detection in the presence of local contrast variation of -30.(a) Original image (b) Forged image (c) Detection result


(a) (b)

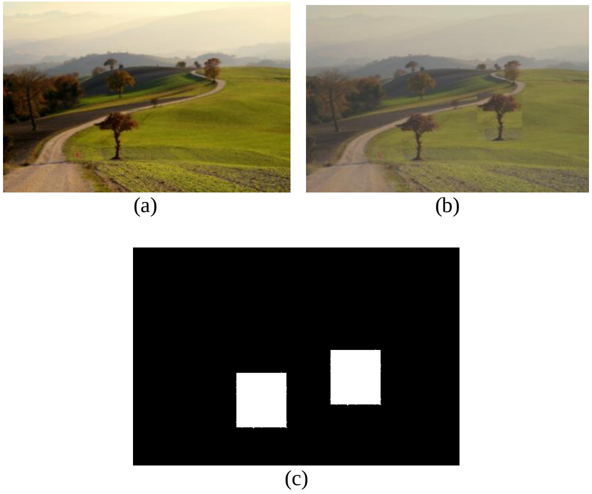
(c)

Fig. 6. Result of forgery detection in the presence of local contrast variation of +40 (a) Original image (b) Forged image (c) Detection result


(a) (b)

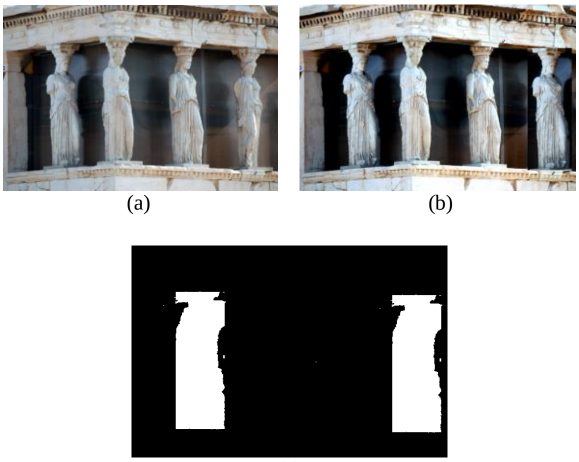
(c)

Fig. 7. Result of forgery detection in the presence of global contrast variation of +50 (a) Original image (b) Forged image (c) Detection result


(a) (b)

(c)

Fig. 8. Result of forgery detection in the presence of global contrast variation of -40 (a) Original image (b) Forged image (c) Detection result



(a) (b)

(c)

Fig. 9. Result of forgery detection in the presence of global contrast variation of +30 (a) Original image (b) Forged image (c) Detection result

V. Conclusion

Different types of post copy move operations are used to deceive the existing image forgery detection techniques. Changing the contrast of the copy moved region or whole forged image is one of such operations. We have proposed a method, which is robust to local and global contrast changes. The method is based on binary DCT coefficients. The forged regions in the images of the dataset have been detected with high detection efficiency in the presence of contrast change. The false detection ratio is very low and the method works with high stability, even in extreme conditions of contrast change. The proposed method has outperformed the compared block based methods in the presence of contrast change. Also, the method is robust to the commonly applied post processing operations like Gaussian noise addition, JPEG compression and minor scaling and rotation. The method may be improved to achieve more rotation and scale invariance.

References

[1] "Image Authentication and Forensics | Fourandsix Technologies - Photo Tampering throughout History." [Online]. Available: http://www.fourandsix.com/photo-tampering-history/. [Accessed: 21-Oct-2014].

[2] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," *Digit. Investig.*, vol. 10, no. 3, pp. 226–245, Oct. 2013.

[3] M. Sridevi, C. Mala, and S. Sanyam, "Comparative Study of Image Forgery and Copy-Move Techniques," in *Advances in Computer Science, Engineering & Applications SE - 71*, vol. 166, D. C. Wyld, J. Zizka, and D. Nagamalai, Eds. Springer Berlin Heidelberg, 2012, pp. 715–723.

[4] S. Kumar, S. Das, and S. Mukherjee, "Copy-Move Forgery Detection in Digital Images: Progress and Challenges.," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 2, pp. 652–663, 2011.

[5] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in *INDIN '05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005.*, 2005, pp. 709–716.

[6] A. Fridrich, B. Soukal, and A. Lukáš, "Detection of copy-move forgery in digital images," *Proc. Digit. Forensic Res. Work.*, 2003.

[7] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," *Dept. Comput. Sci., Dartmouth Coll. Tech. Rep. TR2004-515*, pp. 1–11, 2004.

[8] K. Sunil, D. Jagan, and M. Shaktidev, "DCT-PCA Based Method for Copy-Move Forgery Detection," *Adv. Intell. Syst. Comput.*, vol. 249, pp. 577–583, 2014.

[9] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images.," *Forensic Sci. Int.*, vol. 206, no. 1–3, pp. 178–84, Mar. 2011.

[10] W. Luo and J. Huang, "Robust Detection of Region-Duplication Forgery in Digital Image," *18th Int. Conf. Pattern Recognit.*, pp. 746–749, 2006.

[11] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," *Syst. Signals Image Process. (IWSSIP), 2011 18th Int. Conf.*, pp. 1–4, 2011.

[12] G. L. G. Li, Q. W. Q. Wu, D. T. D. Tu, and S. S. S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries Based on DWT and SVD," *Multimed. Expo, 2007 IEEE Int. Conf.*, pp. 2007–2010, 2007.

[13] Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm for copy-move forgery in digital images," *Forensic Sci. Int.*, vol. 214, no. 1–3, pp. 33–43, 2012.

[14] M. Alsawadi, G. Muhammad, M. Hussain, and G. Bebis, "Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering," *Model. Symp. (EMS), 2013 Eur.*, pp. 249–254, 2013.

[15] R. Davarzani, K. Yaghmaie, S. Mozaffari, and M. Tapak, "Copy-move forgery detection using multiresolution local binary patterns," *Forensic Sci. Int.*, vol. 231, no. 1–3, pp. 61–72, 2013.

[16] S. Bayram, H. Taha Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *2009 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2009, pp. 1053–1056.

[17] G. Lynch, F. Y. Shih, and H.-Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," *Inf. Sci. (Ny).*, vol. 239, pp. 253–265, Aug. 2013.

[18] X. Pan and S. Lyu, "Detecting image region duplication using SIFT features," *IEEE Int. Conf. onAcoustics Speech Signal Process.*, pp. 1706–1790, 2010.

[19] H. Huang, W. Guo, and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," *2008 IEEE Pacific-Asia Work. Comput. Intell. Ind. Appl.*, pp. 272–276, Dec. 2008.

[20] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, and A. Del Bimbo, "Geometric tampering estimation by means of a sift-based forensic analysis," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2010, pp. 1702–1705.

[21] S. Baboo, C. Applications, and C. Forgery, "Detection of Region Duplication Forgery in Digital Images Using SURF," *IJCSI Int. J. Comput. Sci. Issues*, vol. 8, no. 4, pp. 199–205, 2011.

[22] M. Jaberi, G. Bebis, M. Hussain, G. Muhammad, C. Science, and S. Arabia, "Accurate and robust localization of duplicated region in copy-move image forgery," *Mach. Vis. Appl.*, vol. 25, no. 2, pp. 451–475, 2014.

[23] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD-2014; New database for copy-move forgery

detection," *ELMAR, 2013 55th Int. Symp.*, September, pp. 49–54, 2013.

[24] V. Christlein, C. C. Riess, J. Jordan, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *Inf. Forensics Secur. IEEE Trans.*, vol. 7, no. 6, pp. 1841–1854, Aug. 2012.

Authors' Profiles

Sunil Kumar is working as Assistant Professor, Faculty of Engineering & Technology, Mody University of Science and Technology, Lakshmangarh. He has more than 12 years of UG and PG teaching experience after completing his M. Tech. in Computer Science & Engineering in 2002 from Kurukshetra University, Kurukshetra. He has supervised many B. Tech. and M. Tech projects. He has published many research papers in international conferences and journals. He is also reviewer of reputed journals. He is life member of Computer Society of India and current member of IEEE and ACM. His research interest are image forensics, algorithm design and soft computing.

Prof. J V. Desai has completed his PhD form IIT Bombay. He has over 32 years' experience in teaching and research. He is currently Professor and Dean at Mody University of Science and Technology, Lakshmangarh. He has guided 7 PhDs and many M. Tech. scholars. He has published numerous research articles in many international conferences and journals. He has research grants worth many lacs from government and private organizations. He is senior member of many professional bodies like IEEE. He is reviewer of many reputed international journals and conferences. His research interest are Soft Computing, Modeling & Simulation, and Image & Signal Processing.

Prof S. Mukherjee graduated in Electrical Engineering from Patna University in 1968. After having industrial experience for couple of years, he did his Masters in Electrical Engineering from UOR in 1977 and since then is engaged in teaching in UOR and now IIT Roorkee. At present, he is professor and director at Moradabad Institute of Technology, Moradabad and had been Vice Chancellor of Mody Institute of Technology and Science, Rajasthan from 2008 to 2010. He has supervised 7 PhDs and around 35 M. Tech dissertations during his teaching career so far. His areas of interests are system modeling, application of ANN in process control and other areas, order reduction of linear systems along with computer applications in Electrical Engineering. He is senior member of technical societies like IEEE. He is reviewer of many reputed international journals and conferences.

How to cite this paper: Sunil Kumar, J. V. Desai, Shaktidev Mukherjee,"Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors", IJIGSP, vol.7, no.6, pp.38-44, 2015.DOI: 10.5815/ijigsp.2015.06.05