May-June 2020
ISSN: 0193-4120 Page No. 3488-3494

Block Based Technique for Copy-Move Tamper Detection by Means of Image Transformation Technique

[1]V.Thirunavukkarasu, [2]Krishnamurthy R, [3]P.Sathish, [4]J.Satheesh Kumar

[1,2]Assistant Professor, School of Computer Science and Applications, REVA University, Bengaluru
[3]Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore, Tamilnadu, India
[4]Associate Professor, Department of Computer Applications, Bharathiar University, Coimbatore

Article Info
Volume 83
Page Number: 3488-3494
Publication Issue:
May-June 2020

Article History
Article Received: *19 August2019*
Revised: *27 November 2019*
Accepted: *29 January 2019*
Publication: *12 May 2020*

Abstract

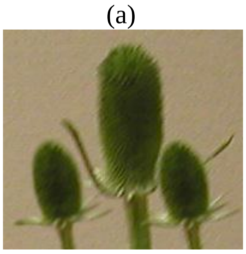
Even though many image tamper detection methods already reported in the literature, still there is a need for developing optimized tamper detection approach due to challenges in the existing methods. This article discusses various image transformation techniques, their applications and limitations. A new block based approach is also introduced in this article. Primary objective of this method is to exactly detect and locate very small and multiple tampered regions even the tampered regions are flipped, enhanced or retouched. The proposed method works better than PCA and DCT based method and overcome the pitfalls in Exhaustive search and Autocorrelation methods which compare every image segment with all other image segment to identify similar region in an image.

Keywords: *copy-move, PCA, DCT, Exhaustive Search, Auto Correlation, accuracy, false- positive*

1. Introduction

Image transformations functions are extensively applied in pre-processing, image compression or data reduction and feature extraction. Images are processed in spatial and frequency domains. In Spatial domain image pixels are directly processed which incurred more computation which makes the image processing task a complex one [1][2]. Frequency domain methods transform the image in to frequency domain and perform operations on transformed image. After processing, the image is transformed back to original image by means of inverse transform. Transformation function provides some additional or hidden information and it is easy to solve than the original function. Figure 1 illustrates copy-move manipulation [3][4] .

(a)



(b)

Figure 1: (a) Original Image (b) Manipulated image

2. Literature Review

Fridrich et al introduced the method by means of Discrete Cosine Transformation to detect a special type of tampering called copy-move. Suspected image is alienated to overlaid chunks than DCT transformation has employed with all blocks. Quantized co-efficient are lexicographically sorted to effectively match the identical blocks. This process has higher processing complexity and produce false matches in the uniform and flat areas of the image [5]. Zhouchen et al. used an automatic tamper detection method that discover altered JPEG images by investigating the double quantization consequence concealed along with the DCT co-efficient. This method is efficient even when the altered segment is post-processed with diverse techniques like in-painting, texture synthesis and alpha matting. Comparing with existing methods accuracy of this method is low and fails to detect some tampered image. The feature dimensions of this method will cause processing difficulty [6]. Bravo et al projected a modus operandi with Log polar transformation. This process used to diminish the magnitude of feature descriptor. It is suitable to perceive manipulated fragment that is rotated, scaled and translated. However, the method is not appropriate for tampered image which is tainted by additive noise and JPEG compression. Log-polar transformation technique is more complicated than DCT technique [7].Qiumin et al. employed a technique that uses Log-Polar Fast Fourier Transform on image chunk to ballpark the Log-Polar Fourier Transformation. The extracted features are fine structured to fit in to computer memory to ensure optimum feature extraction. To compute discrete Fourier transform for all the blocks of an image leads high computational complexity [8].

3. Role of Transformation in Tamper Detection

Various transformation methods have already in use. Few important transformation techniques have been discussed as follows

3.1 Fourier Transform

It expresses non-periodic and even functions with finite durations as an integral of sines / cosines proliferated with a weighting function. Fourier transformation function is completely recovered reverse to the spatial domain in the course of inverse process without loss of any information. Discrete Fourier Transforms (DFT) exposes periodicities and strength of periodic components in the input signals. In DFT independent variables are discrete and always there exist an inverse for forward DFT.

3.2 Walsh Transform

It is a real transform consist series expansion for basic utility whose values are +1 or -1 hence, it necessitate fewer memory than Fourier transform. Walsh transformation is mainly used in multiplexing, in which several data is simultaneously transmitted without the need of high energy packing capability.

3.3 The HADAMARD Transform

It is well suited for digital signal processing because the basic vector is obtains merely the values +1 and -1. Therefore no multiplications are required in the transform calculation. It is real, symmetric and orthogonal transform which reduce number of additions and subtractions from N^2 to $N\log_2 N$. Recursive relation is an important property in which HADAMARD matrix of any magnitude is calculated from the tiny initial HADAMARD matrix.

3.4 The HAAR Transform

It is real, orthogonal and fast transform on N X 1 vector. It can be implemented in O (N) operations. The basic vectors of HAAR matrix are sequentially ordered and used for image edge extraction. This transform exhibit poor energy compaction for images therefore it is not much useful in practice.

3.5 The SLANT Transform

SLANT transform is developed for monochrome or color image coding. Quality of an image coded by SLANT transform is higher than other unitary transform coded images. It is real, orthogonal and fast transforms which can be implemented in O ($N\log_2 N$) operations on an N X 1 vector. Even though it has better energy compaction property than HAAR transform it is not used in practice.

3.6 KARHUNEN LOEVE (KL) or HOTELLING Transform

It is also notorious as eigenvector transform or method of principal components or Discrete KL transform. It depends on the algebraic properties of vector depiction It is very important tool used to evaluate performance and finding performance bounds in image data.

All transformations discussed in the above section have low energy compaction, de-de-correlation property which leads the possibility for redundant data and bundle of energy is associated with many coefficients.

3.7 Discrete Cosine Transform (DCT)

DCT is the best suitable method to address various issues discussed in previous section. An interesting contribution in this exertion is the design and development of new tamper discovery method using DCT. The Cosine transform is a fast transform mainly used in image compression. This mathematical transformation technique employed to convert the image from spatial domain to frequency domain and attempt to de-correlate the image pixels subsequent to every transform co-efficient are fixed separately. Since DCT kernels are separable and orthogonal the 2D forward and inverse transform is calculated by consecutive application of 1D-DCT co-efficient [9].

3.7.1 One dimensional DCT

The one dimensional DCT coefficients are deliberated with the formula,

$$h(c) = \lambda(c) \sum_{u=0}^{NE-1} g(u) \cos\left(\frac{(2u+1)c\pi}{2NE}\right) \quad (1)$$

Where u=0, 1, 2…N-1 and

May-June 2020
ISSN: 0193-4120 Page No. 3488-3494

$$\lambda(c) = \begin{cases} \sqrt{\frac{1}{n}} & \text{for} \quad c = 0 \\ \sqrt{\frac{2}{n}} & \text{for} \quad c = 1,2,\ldots,NE-1 \end{cases}$$

c(u) illustrates one dimensional DCT coefficients

3.7.2 Two dimensional DCT

The 2D-DCT is illustrated as,

$$h(c,d) = \lambda(c)\lambda(d) \sum_{c=0}^{NE-1} \sum_{d=0}^{NE-1} f(c,d) \left[\cos\left(\frac{(2c+1)c\pi}{2NE}\right) \cos\left(\frac{(2d+1)d\pi}{2NE}\right) \right] \quad (2)$$

Where u=0, 1, 2….N-1 and v=0, 1, 2…..N-1 and

$$\lambda(c) \text{or}\, \lambda(d) = \begin{cases} \sqrt{\frac{1}{n}} & for \quad c\ (\text{or})\ d = 0 \\ \sqrt{\frac{2}{n}} & for \quad c\ (\text{or})\ d = 1,2,..NE-1 \end{cases}$$

h(c, d) is portrayed two dimensional DCT coefficients

4. DCT Based Tamper Detection using Sub Block Approach

Architecture of proposed tamper detection method is shown in figure 2.

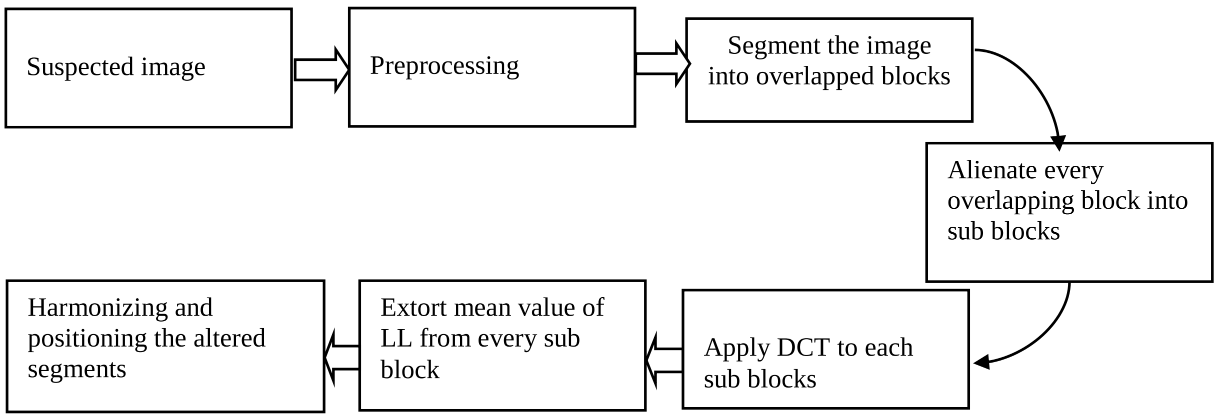


Figure 2: Frame work of proposed tamper detection algorithm

Step 1: Pre-processing: **T**he alleged image AI is checked as gray scale or colour image. If it is colour than it is converted in to gray scale with the formula,

AI = 0.299 R + 0.587 G + 0.114 B (3)

Step 2: Pre-processed image is alienated with overlie chunk of rigid magnitude b X b. Every neighbouring block will have one dissimilar row and column. Magnitude of the overlapping blocks should not exceed the size of the assumed tampered region thus the block size is optimized by performing series of experiments with different arbitrary tampered image regions and comparing exiting state of art methods. After series of experiments and comparisons block size is fixed as 8 X 8. Each overlapping blocks are represented by OB_{ij} where i and j indicates starting position of row and column of a particular block. Total number of overlapping blocks should not exceeds (M-b+1)(N-b+1). Where M, N denotes the size of the input image and b denotes the block size.

Step3: Each overlaid chunk of magnitude b X b is further alienated into non-overlaid chunk of magnitude NB X NB.

Step 4: The 2D-DCT is enforced to every non-overlaid chunks.

Step 5: The mean value of low frequency DCT component from each sub chunk is acquired and arranged as two dimensional matrix (MatLF). Each row contains one block coefficients. Lexicographical sorting is employed to compare the resemblance among blocks. As a result, similar rows are adjacent to each other which help to locate the tampered regions. Flowchart for lexicographical sorting is shown in figure 3.

TEST Engineering & Management

May-June 2020
ISSN: 0193-4120 Page No. 3488-3494

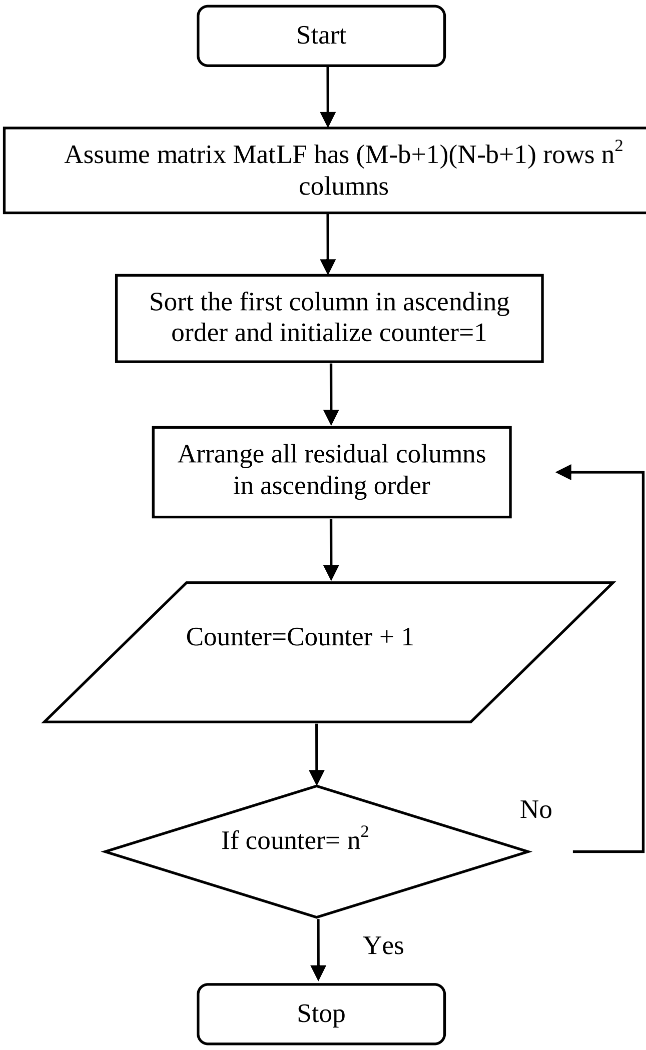


Figure 3: Flowchart of lexicographical sorting

Step 6: Every row in the matrix MatLF is matched with all other rows in order to recognize similar image chunks. The shift vector (SH) is deliberated for similar rows using the formula,

$SH = (SH1, SH2) = (i1 - j1, i2 - j2)$ (4)

False discovery is detached by fixing the (T).

5. Experimental Analysis

Projected technique is implemented in Mat lab R2018b. Images used in this experiment are acquired from three diverse datasets. First dataset embrace 10 images of scale 200 X 200 pixels produced by Muhammad et al [10]. The second data set is Kodak image data set introduced by Kodak Corporation which contains 24 images of scale 768 X 512 pixels available for unrestricted research purpose [11]. The last data set which includes PNG images of dissimilar magnitude [12]. The discovered outcome of projected technique is exemplified in figure 4, figure 5 and figure 6.

(a) (b) (c)

(d) (e) (f)

Figure 4: Discovered result of simple copy-move manipulation (a) and (d) original images, (b) and (e) Manipulated images, (c) and (f) Discovered results using DCT approach

(a) (b) (c)

Figure 5: Discovered outcome of multiple copy-move tampering (a) Authentic image, (b) Multi tampered image, (c) Discovered result

(1) (2) (3)

Figure 6 (a): Detection result of copy-move with flipping (1) original image (2) Tampered image with flipping (3) Detection result

Performance of new block based tamper detection algorithm is analysed in image and pixel levels. Image level analysis helps to identify it is manipulated or not. Pixel level analysis demonstrates, how precisely the technique perceive manipulated area. Diverse measurements such as Precision, Recall, F1 measure, Accuracy, and False Positive Rate are utilized to estimate the performance.

The metric precision, recall and F are discussed in chapter 2. Accuracy is used to evaluate how well the method will locate the tampered region. It is calculated using the formula,

$$\text{Accuracy} = \frac{|\rho \cap \rho^{T}| + |\lambda \cap \lambda^{T}|}{|\rho| + |\lambda|} \quad (5)$$

Where, ρ and λ indicates the pixels of authentic and tampered segments of tampered image. ρ^{T} and λ^{T} specifies the pixels of Authentic and tampered segment of discovered resultant image, ∩ indicates the intersection of two regions.

$$FDR = \frac{|\rho^{T} - \rho| + |\lambda^{T} - \lambda|}{|\rho^{T}| + |\lambda^{T}|} \quad (6)$$

Where, FDR reveals the amount of pixels which are not enclosed in manipulated region but wrongly incorporated by the proposed technique and – indicates the difference of two regions. Table 1 illustrate the performance of this method.

6. Performance Comparison

Performance of the block based approach is assessed with two methods such as Fridrich et al [1] and popescu et al [13] methods. Image manipulation dataset is used for this intention, which restrains 48 authentic and 48 manipulated images of diverse magnitude. The metrics precision, recall and F measure are used to compare simple copy-move tampering at image level and the detection results are compared as shown figure 7.

Table 1: Performance of proposed block based approach

Image	Size	Precision	Recall	F1	Accuracy	FPR
Giraffe	800 X 533	80.78	69.39	74.65	99.38	0.002
Box image	200 X 200	91.77	100	95.70	98.40	0.005
Hat	768 X 512	90.73	98.65	94.52	97.67	0.007
Leaves group	200 X 200	96.08	80.01	86.97	99.17	0.001

Images are grouped in to three categories such as nature, manmade and mixed and their detection results are compared in the figure 8. Further the images are categorized into three types such as smooth, rough, structured based on their texture properties and their detection results are shown in figure 9. Proposed technique outperforms the two methods with different image categories in terms of precision, recall and F measure.

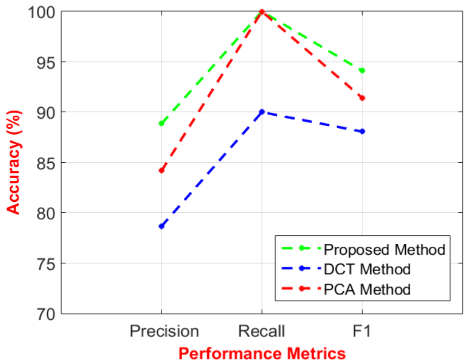


Figure 7: Average detection accuracy of simple copy-move tampering

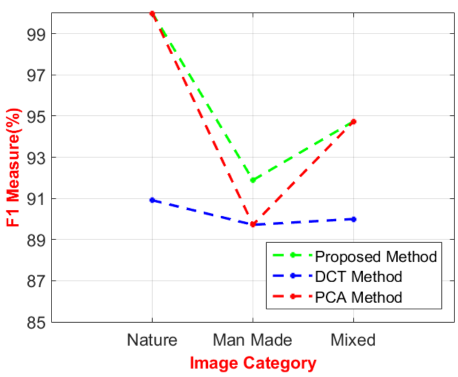


Figure 8: Average detection accuracy (F) based on image category

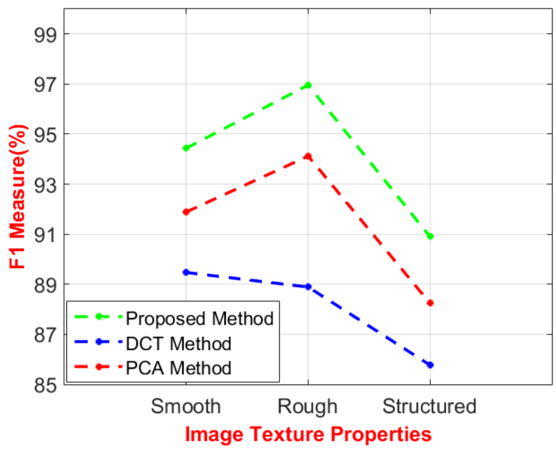


Figure 9: Average detection accuracy (F) based on image texture properties

7. Conclusion

Various block based approach have been projected to perceive copy-move tampering however, developing a technique that repeatedly perceive and position the tampered area with high accuracy and low false positive rate without any embedded code or watermark is a challenging task in image processing. This article reviewed different image transformation techniques and its significance. The proposed block based technique precisely discovers and locates very tinny and multiple tampered regions under the different distortions like flipping enhancement and retouching. This method works better than PCA and DCT based methods in terms of precision, recall and F measure.

8. Acknowledgment

The authors would like to thank Vision Group of Science and Technology (VGST), Government of Karnataka, India for their financial support under the RGS/F grant (Grant No: KSTePS/VGST-RGS/F/GRD No.695/20L7).

References

[1] V. Thirunavukkarsu, J. Satheesh Kumar, “A novel method to detect copy-move tampering in digital images”, IND-JST, 9(8), pp:1–4, 2016

[2] V. Thirunavukkarasu, J. Satheesh Kumar, Gyoo Soo Chae, J. Kishorkumar,| “Nonintrusive Forensic Detection Method Using DSWT with Reduced Feature Set for CopyMove ImageTampering”, Wireless Personal Communications, Springer, pp:1-19

[3] V.Thirunavukkarasu, J.Satheeshkumar, “Passive Image Tamper Detection Based on Fast Retina Key point Descriptor”, IEEE-ICACA, pp.279-285, 2016

[4] V.Thirunavukkarasu, J.Satheesh Kumar, “Evolution of Blind Methods for Image Tamper Detection-A Review”, **IJAER**, Vol. 9 (21), 2014, pp. 5069-5076.

[5] Fridrich A, Jessica B, David Soukal, A. Jan Lukas, “Detection of copy-move forgery in digital images”, In Proceedings of Digital Forensic Research Workshop, 2003.

[6] Zhouchen Lina, JunfengHeb, XiaoouTanga, Chi-KeungTang, “Fast, automatic and finegrained tampered JPEG image detection via DCT coefficient analysis”, Pattern Recognition, Vol.4 (2), pp: 2492 – 2501, Elsevier, 2009

[7] Bravo-Solorio, A.K. Nandi, “Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling”, European Signal Processing Conference (EUSIPCO 2009), pp: 824–828, 2009

[8] Qiumin Wu, Shuozhong Wang, and Xinpeng Zhang, “Log-Polar Based Scheme for Revealing Duplicated Regions in Digital Images”, IEEE signal processing letters, Vol. 18(10), pp: 559-562, 2011.

[9] R. Gonzalez and R. Woods, 2002 “Digital Image Processing” 3rd Edn., Prentice Hall Publication, ISBN:9788120336407

[10] Muhammad G, Hussain M, Khawaji K, Bebis G, “Blind copy move image forgery detection using dyadic un-decimated wavelet transform”, Digital signal processing, pp:1-6, 2011.

[11] Kodak Lossless True Color Image Suite: http://r0k.us/graphics/kodak

[12] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, Elli Angelopoulou, “An Evaluation of Popular Copy-Move Forgery Detection Approaches”, IEEE International transactions on information forensics and security, vol.2(4), PP:1-26, 2012.

[13] A. Popescu, H. Farid, “Exposing digital forgeries by detecting duplicated image regions”, Technical Report TR2004-515, Department of Computer Science, Dartmouth College, 2004