Advanced Research in Electrical and Electronic Engineering
Print ISSN: 2349-5804; Online ISSN: 2349-5812 Volume 1, Number 3 (2014) pp. 76-81

http://www.krishisanskriti.org/areee.html

Computationally Efficient Copy-Move Image Forgery Detection Based on DCT and SVD

Kavya Sharma

Dept. of ECE, N.I.T. Kurukshetra, (Haryana)- INDIA

Abstract: **Most of the existing techniques perform detection of Copy-Move forgery by extracting large feature vectors causing heavy computation. Here, we propose a block based method for detection of copy move forgery in which extracted feature vector from each block is of very small size containing only four elements. In this method, an image is divided into overlapping blocks of fixed size then DCT and SVD are used to extract feature vectors from each block. Duplicated regions are then detected by lexicographically sorting feature vector of all the image blocks. Experimental results show that proposed method can effectively detect multiple copy-move forgery and precisely locate the duplicated regions even when an image has undergone common post processing operations like Gaussian blurring, AWGN, JPEG compression and their mixed operations.**

1. INTRODUCTION

Increased popularity and availability of powerful digital image editing tools made it easy for almost anyone to create, alter and manipulate digital images with no obvious traces of any of these operations. As digital images are widely used in various fields like forensic investigation, law enforcement, surveillance systems, medical imaging, journalism and military therefore developing techniques to detect image tampering has become main concern of image forensics, since it may no longer be possible to distinguish whether a given digital image is original or a modified version.

(a) **(b)**

Fig.1. Example image of a typical copy-move forgery. Left image is the original image and Right image is the tampered image.

A specific type of forgery, which is the main interest of this paper is copy-move forgery. Copy-move forgery is most common tempering technique which is generally done to conceal the unwanted region of an image and thus creating a misleading image. To detect copy-move forgery, detection method should be able to identify the tempered image and precisely locate duplicate regions. As the duplicated regions comes from same image thus have similar property e.g. texture, color, noise etc. Up till now, many passive detection techniques have been proposed to detect copy-move forgery. Fridrich first proposed a direct approach to detect region duplication forgery based on exhaustive search [1]. But due to its high computational complexity it is not used for practical applications. Block-matching is proposed to reduce the computation complexity. In block based methods image is divided into overlapping or non-overlapping blocks and different operations are applied on those blocks to extract feature vector from those blocks. Fridrich et al. [1] also proposed a block based method using Discrete Cosine Transform (DCT) and lexicographic sorting. Popescu and Farid [2] proposed performing Principal Component Analysis (PCA) to extract a representation of each image block. Luo et al. [3] proposed color features and the block intensity ratio in four directions of the image to detect copy-move forgery. Li [4] proposed to extracted features of the circular blocks by using local binary patterns. J. Zhao and J Guo [5] proposed a robust method based on DCT and SVD. Lexicographic sorting is used to detect duplicated image blocks. The primary cost of this algorithm is the lexicographic sorting, yielding a complexity of O(mn log n), where m denotes the size of feature vector and n is the number of image blocks, which is proportional to the number of image pixels. In most of existing methods feature vectors are large in size causing high computation. In this paper we propose an improved version of copy-move image forgery detection technique based on DCT and SVD [5] which is computationally efficient and give comparable performance. In our experiments we extracted a feature vector of four elements thus computations involved reduces.

The rest of the paper is organized as follows. A brief description of DCT and SVD is given in Section 2. In Section

3, the proposed method is described in detail. The experimental results and the corresponding analysis are given in Section 4. The conclusion is drawn in Section 5.

2. DCT AND SVD

2.1. Discrete cosine transform

Discrete Cosine Transform (DCT) is a mathematical transform, applying DCT on an image gives DCT coefficient in frequency domain for each pixel of image in spatial domain. DCT is important to various applications in science and engineering, it is used for lossy compression of image (i.e. JPEG) and audio (i.e. MP3), also used in spectral methods for numerical solutions of partial differential equations. DCT has strong energy compaction property which causes most of signal energy to be concentrated in few low frequency components of the DCT. Other useful properties of DCT are de-correlation and symmetry. These properties are important for image processing. 2-D DCT of M×N matrix is defined as follows,

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \quad (1)$$

Where, $0 \leq p \leq M-1$, $0 \leq q \leq N-1$

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, p = 0 \\ \frac{\sqrt{2}}{M}, 1 \leq p \leq M-1 \end{cases}, \alpha_q = \begin{cases} \frac{1}{\sqrt{M}}, q = 0 \\ \frac{\sqrt{2}}{M}, 1 \leq q \leq M-1 \end{cases}$$

Where B_{pq} is the DCT coefficient of grayscale value A_{mn}. When 2-D DCT is applied on a block of image it gives DC and AC coefficients, most of the high frequency coefficients are insignificant only DC term and some low frequency AC coefficients are significant.

2.2 Singular Value Decomposition

SVD is a factorization of a matrix. Let A be an image matrix with A$\in R^{M\times N}$ of rank r, its SVD is given by the formula

$$A = U \sum V^T \quad (2)$$

where U is a $M \times M$ matrix of orthonormal eigenvectors of AA^T, V is a $N \times N$ matrix of orthonormal eigenvectors of $A^T A$. $\sum$ is a $M \times N$ diagonal matrix containing square roots of eigen values of $A^T A$.

$$\Sigma = \begin{bmatrix} \Sigma_r & 0 \\ 0 & 0 \end{bmatrix} \quad (3)$$

Where Σ_r is a square diagonal matrix in $R^{r\times r}$. Diagonal entries of Σ_r are called singular values of A. Σ_r can be defined as, $\Sigma_r = diag(\sigma_1, \sigma_2, \sigma_3, \ldots\ldots, \sigma_r)$, where ($\sigma_1 \geq \sigma_2 \geq \sigma_3 \geq \ldots\ldots \geq \sigma_r) > 0$. SVD has three main property scaling property, stability and rotation invariance. SVD has various applications in field of signal processing, data compression and pattern analysis. It can be used for dimensionality reduction and also for noise reduction. Shift vectors are unique for a matrix and can be grouped into two groups, large and small values. Relatively small values are sensitive to noise, whereas large singular value (LSV) contains most energy of each image block. LSV has good stability against some minor distortions.

3. PROPOSED METHOD

In the case of copy-move forgery, task of detection technique is to find and locate the pair of similar regions in the tempered image. As shape and size of duplicated region is unknown, comparing each possible pair of blocks pixel by pixel will be very complex and need high computation. Thus in the proposed method feature extraction from each block is done by using DCT and SVD. Energy compaction property of DCT makes use of smaller feature vector possible to detect duplicate regions. Fig. 2 shows steps involved in proposed method.

3.1. Implementation steps

Step 1: Pre-processing the suspicious image.

Assume input image is a gray image of size M×N. if input image is a color image we convert it into a grayscale image by using standard formula,

Fig.2. Steps for detection of copy-move forgery

Y = 0.299R + 0.587G + 0.114B (4)

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

Step 2: Division of input image into overlapping blocks.

Suspected image is divided into b×b overlapping blocks by sliding one pixel from top left corner down to bottom right corner of the image, so that adjacent overlapping blocks will

only have one different row or column. Each block is denoted by B_{ij}, where i and j denotes the starting point of the block's row and column respectively. It is assumed that size of duplicated region is larger than the size of block.

Step 3: 2D-DCT and Quantization

To each block two-dimensional DCT is applied, which gives DCT coefficient matrix of same size. Than this coefficient matrix is quantized by using JPEG quantization table (as the size of standard quantization matrix is 8×8 thus here block size is also taken as 8×8). Quantization is performed to obtain more robust representation of image block. Quantized DCT coefficient can be obtained by formula defined as,

$$D_{ij}^{q} = round(\frac{D_{ij}}{Q_{ij}}), \text{ i, j} = 0,1,2\ldots..,7 \quad (5)$$

here D_{ij} is the un-quantized DCT coefficient, Q is the quantization matrix and D_{ij}^{q} is the quantized coefficient.

Step 4: Concatenation of quantized coefficient matrix.

According to the property of DCT, the energy of signal will be concentrated over low frequency coefficients, thus all the elements will not be equally important. The top left part of DCT coefficient matrix represents most of information. Applying quantization on coefficient matrix will produce a matrix, in which except few low frequency elements all other elements will be zero. Thus we can eliminate these zero value element as they do not provide any additional information about the corresponding image block. By experimentation it is concluded that a 4×4 matrix taken from top left corner of quantized matrix is sufficient to represent a block for detection of forged region. Let each 4×4 concatenated block be denoted by Z_{ij}.

Step 5: Division into sub-blocks and Extracting feature vector

Each concatenated block Z_{ij} is divided into non overlapping 2×2 sub blocks. SVD is applied to each sub block and LSV of each sub block is obtained. For each quantized block, there will be 4 LSV's corresponding to different sub blocks. These LSV's constitute a feature vector to represent a block, let S_{maxp} is the LSV corresponding to p^{th} sub block where, $p \in \{1,2,3,4\}$. Then feature vector of size 1×4 can be denoted as,

$$V = [S_{max1}, S_{max2}, S_{max3}, S_{max4}] \quad (6)$$

Step6. Matching of similar block pair

Feature vector for each block is obtained and a matrix A is created arranging feature vectors into feature matrix. As for an image of size M×N, there will be (M-b+1)(N-b+1) blocks of size b×b, so matrix A is of size (M-b+1)(N-b+1)×4, each row corresponds to feature vector of a block.

$$A = \begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ \vdots \\ V_{(M-b+1)(N-b+1)} \end{bmatrix} \quad (7)$$

Note that for duplicate block pair in image there feature vectors will be similar as well, thus we need to find matching feature vectors. For this we lexicographically sort the rows of A to make feature vectors of matching blocks adjacent to each other. To avoid false matches, if 2 adjacent rows of lexicographically sorted matrix $\tilde{A}$ are found similar, a shift vector is calculated between them. The location of respective blocks is stored in a separate list. Algorithm output a block pair only if there are many other matching pair with same shift vector. Shift vector S between 2 blocks can be calculated as,

$$S = (s_1, s_2) = (i_1 - i_2, j_1 - j_2) \quad (8)$$

Where $(i_1, j_1), (i_2 j_2)$ are the co-ordinates of top left corners of the blocks corresponding to adjacent shift vectors in A. As shift vector –S and S corresponds to same shift, it is normalized so that S≥0. For each pair of block, we increment corresponding normalized shift vector counter by one.

$$C(s_1, s_2) = C(s_1, s_2) + 1 \quad (9)$$

value of C is taken as zero in starting of algorithm, C indicates the frequency of occurrence of different normalized shift vectors. Then we compare shift vector counter value of all shift vectors with a threshold T_{shift} and choose shift vectors, $s_1, s_2, \ldots \ldots s_k$, whose occurrence exceeds this threshold.

$$C(S_r) \geq T_{shift}, \text{ for all r=1, 2,…, k} \quad (10)$$

Value of this threshold is related with the size of smallest region that can be identified by algorithm. Another user specified threshold T_d is used to specify minimum distance between duplicated regions. It is assumed that duplicated regions are not overlapping and blocks being compared may be overlapping. Thus for two similar feature vector, shift vector is calculated only if Euclidean distance between them is greater than T_d.

$$\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} > T_d \quad (11)$$

If the test satisfies equation (10) and (11), we mark a color map for copied and duplicated blocks to represent the forgery detection result.

Step7: Post-Processing and output

Morphologically open operation is applied. It fills the holes in marked regions and removes isolated blocks. Its output is the final detection result.

4. EXPERIMENTAL RESULTS

All the experiments were carried out on the platform intel core i3 processor 2.26 GHz and MATLAB R2008a. Images are collected from two databases [6, 7]. The first dataset contains some images from the miscellaneous volume of USC-SIPI database with the sizes of 256×256 pixels and 512×512 pixels [6]. The second dataset contains 24 uncompressed PNG true color images of size 768×512 pixels released by Kodak Corporation for unrestricted research usage [7]. In our experiment all the parameters are set as: b=8, Q=75, T_d=40, T_{shift}=90 by default. For morphological opening a disk of radius 5 is used.

4.1. Qualitative Evaluation

A copy-move detection technique should correctly identify weather an image is tempered or not and must be able to locate the forged region. Detection performance was evaluated on image level in terms of Precision, p and Recall, r. For calculating these measures we need to keep a record of the number of correctly detected forged images T_P, the number of images falsely detected as forged images F_P and number of falsely missed forged image F_N. p and r are calculated as,

$$p = \frac{T_P}{T_P + F_P} \quad (12)$$

$$r = \frac{T_P}{T_P + F_N} \quad (13)$$

Precision gives the probability of an image detected as forged is truly forged, and Recall is the probability of detecting a forged image.

We also evaluated our algorithm on pixel level that gives how correctly it can locate the forged region. Two measures are used for this, detection accuracy rate, DAR and the false positive rate, FPR. They are calculated as,

$$DAR = \frac{|\psi_S \cap \tilde{\psi}_S| + |\psi_T \cap \tilde{\psi}_T|}{|\psi_S| + |\psi_T|} \quad (14)$$

$$FPR = \frac{|\tilde{\psi}_S - \psi_S| + |\tilde{\psi}_T - \psi_T|}{|\tilde{\psi}_S| + |\tilde{\psi}_T|} \quad (15)$$

where ψ_S, ψ_T denotes pixels of original region and forgery region in original image respectively and $\tilde{\psi}_S, \tilde{\psi}_T$ denotes pixels of original region and forgery region in detected output image respectively. $|\ |$ means the area of region, $\cap$ means the intersection of two regions and – means the difference of two regions. DAR give the performance of algorithm at correctly locating pixels of copy-move regions in the tempered images and FPR gives the percentage of pixels which are not contained in duplicated region but included by detection algorithm. For an efficient and precise method DAR must be close to 1 and FPR should be close to 0.

4.2. Effectiveness and accuracy test

To test the effectiveness of our algorithm we selected some color images with the size of 768×512 pixels from the second dataset. In the images, we randomly choose blocks with two sizes, 32×32 pixels and 64×64 pixels to tamper with. Corresponding detection results are illustrated in Fig. 3. The top row shows the tampered images, where yellow lines indicates the copy-move regions and pasting location, and the bottom row shows the detection results.

DAR=1, FPR=0 DAR=1, FPR=0

32 pixels × 32 pixels 64 pixels × 64 pixels

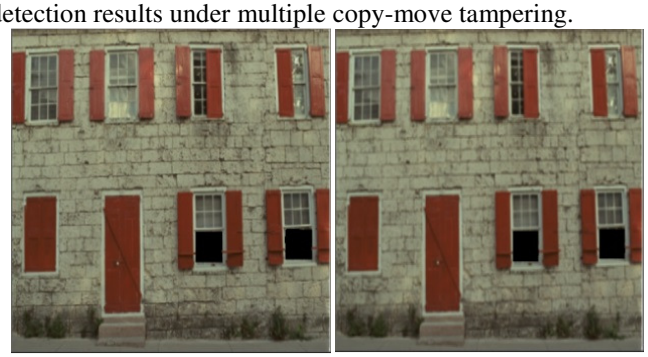
Fig. 3. Shown on the top row are two tampered images with different sizes of duplicated regions. Below them are the corresponding detection results. DAR/FPR rates and size of duplicated regions are given respectively.

(a) (b) (c)

Fig. 4. Shown are the tampered images with non-regular copy-move forgeries.

4.3. Robustness test

Generally forgery makers do different post-processing operations to make an imperceptible tempered image. There are various post processing operations e.g. Gaussian blurring, jpeg compression, AWGN. In order to evaluate the robustness of our algorithm against different image distortions, we selected randomly 50 original images from the 2 datasets to generate tampered images by copying a square region from a random location and pasting onto a non-overlapping region. The sizes of square region were 32×32 pixels and 48×48 pixels respectively. On each image copy-move forgery is done with four different relative locations to generate 400 tampered images. Some more tampered images are generated in which the duplicated regions are non-regular and meaningful objects. Then these tampered images and their original version were distorted by commonly used post-processing operations with different parameters, such as Gaussian blurring, AWGN and JPEG compression and mixed operations. Fig. 4 shows three tampered images with non-regular copy-move forgery. Fig.5-6. shows detection results of copy-move forgeries with different post processing operations. Fig. 7 shows the detection results under multiple copy-move tampering.



DAR=0.8911, FPR=0 Gaussian blurring (w=5,σ = 1)

DAR=0.8689, FPR=0 Gaussian blurring (w=5,σ = 3)

DAR=0.8452, FPR=0.183 AWGN (SNR=25dB)

DAR=0.8458, FPR=0.182 AWGN (SNR=30dB)

DAR=0.904,FDR=0.105 JPEG compression (Q=65)

DAR=0.960,FDR=0.040 JPEG compression (Q=75)

Fig. 5. Shown are the detection results of copy-move forgeries under multiple post-processing operations. DAR/FPR rates are given below respectively.

The experimental results of evaluation for robustness from image level and pixel level respectively were given in Tables 1–3. The detection results shown in Tables 1–3 indicate that detection performance of our method is similar to previous method[5].

Table 1. Detection results of the tampered images distorted by Gaussian blurring.

	w=3, σ=0.5		w=3, σ=1		w=5, σ=05		w=5, σ=1	
	32x32	48x48	32x32	48x48	32x32	48x48	32x32	48x48
p	0.999	1.000	0.990	0.996	0.983	0.990	0.980	0990
r	1.000	1.000	1.000	1.000	0.990	1.000	0.986	1.000
DAR	0.927	0.946	0.887	0.930	0.909	9.47	0.846	0.890
FPR	0.035	0.018	0.30	0.17	0.029	0.010	0.052	0.016

Table 2. Detection results of the tampered images distorted by AWGN.

	SNR=40db		SNR=35db		SNR=30db		SNR=25db	
	32x32	48x48	32x32	48x48	32x32	48x48	32x32	48x48
p	1.000	1.000	0.986	0.990	0.970	.981	0.965	0.975
r	1.000	1.000	0.990	1	0.977	.980	0.930	0.934
DAR	0.990	0.996	0.982	0.992	0.953	.966	0.890	0.892
FPR	0.005	0.005	0.014	0.042	0.071	.104	0.161	0.158

Table 3. Detection results of the tampered images distorted by JPEG compression

	Q=90		Q=80		Q=70	
	32x32	48x48	32x32	48x48	32x32	48x48
p	0.946	0.969	0.907	0.934	0.879	0.894
r	0.970	0.974	0.920	0.939	0.823	0.876
DAR	0.964	0.979	0.881	0.939	0.779	0.817
FPR	0.012	0.003	0.081	0.008	0.135	0.024

COMPUTATIONAL COMPLEXITY TEST

The complexity of this algorithm, dominated by the lexicographic sorting is O (mn log n), where m denotes the size of feature vector and n is the number of image blocks, which is proportional to the number of image pixels. Table 4, Shows that number of computations involved reduces by a factor of 4 as in the proposed method size of feature vector is reduced 4 times in comparison to DCT and SVD method[5].

DAR=0.763, FDR=0.309
AWGN (SNR = 25) +
Gaussian blurring (w = 3, σ = 1)

Fig.6. Shown is the detection result of copy-move forgery under multiple post processing operations. DAR/FPR rates are given below respectively.

DAR=0.999, FDR=0

Fig.7. Shown is the detection result of multiple copy-move forgery. DAR/FPR rates are given below respectively.

Table 4. Reduction in computations

Image size	DCT and SVD method	Proposed method
	No. of computations (in lakhs)	
256x256	47.54	11.88
512x512	220.061	55.15
768x768	533.974	133.49

5. CONCLUSION

We have proposed an improved version of copy-move image forgery detection technique based on DCT and SVD [6] which is computationally efficient and give comparable performance. Compared with previous works less no. of computations are needed as size of feature vector is smaller. The experimental results show that the proposed algorithm is computationally efficient and provide similar results in terms of effectiveness to detect multiple copy-move forgery and precision to locate the duplicated regions. It also has robustness to Gaussian blurring, AWGN, JPEG compression and their mixed operations. Overall performance of our method is better.

REFERENCES

[1] J. Fridrich, D. Soukalm, J. Lukas, "*Detection of Copy-Move Forgery in Digital Images"*, Digital Forensic Research Workshop, Cleveland, 2003, pp. 19–23.

[2] A.C. Popescu, H. Farid, "*Exposing Digital Forgeries by Detecting Duplicated Image Regions"*, Tech. Rep. TR2004-515, Dartmouth College, 2004.

[3] W. Luo, J. Huang, G. Qiu, *"Robust detection of region-duplication forgery in digital images*", in: International Conference on Pattern Recognition, Vol. 4, 2006, pp. 746–749.

[4] L. Li, S. Li, H. Zhu, *"An efficient scheme for detecting copy-move forged images by local binary patterns*", J. Inf. Hiding Multimedia Signal Process. 4 (1) , 2013, pp. 46–56.

[5] Jie Zhao and Jichang Guo, "*Passive forensics for copy-move image forgery using a method based on DCT and SVD*", Forensic Science International 233, 2013, pp. 158–166.

[6] The USC-SIPI Image Database: http://sipi.usc.edu/database/.
Kodak Lossless True Color Image Suite: http://r0k.us/graphics/kodak/.