International Journal of Computer Applications (0975 – 8887)
Volume 88 – No.8, February 2014

Copy –Move Forgery Detection using Orthogonal Wavelet Transforms

Tanuja K. Sarode, Ph.D
TSEC, Bandra
Mumbai

Naveen Vaswani
WIEECT, Worli
Mumbai

ABSTRACT
With the help of various image editing tools available, it has become easier to alter an image in such a way that it does not leave behind any clues. Copy –Move forgery is a type of image forgery in which a part of digital image is copied and pasted to another part of same image. Since the copied and pasted image comes from the same image, it becomes difficult to detect the forgery. Generally the intention behind Copy-Move forgery is to hide important objects in an image. In this paper, an orthogonal wavelet transform based forgery detection method is proposed. Orthogonal wavelet transform is generated from basic orthogonal transforms. We consider generating Discrete Cosine Transform Wavelet (DCTW) transform and Walsh Wavelet (WW) transform from DCT and Walsh orthogonal transforms. The image is divided into overlapping blocks. On each block, DCTW and WW transforms are applied. From each block discriminative features are extracted from coefficients. These feature vectors are lexicographically sorted and block matching step is applied to find duplicated blocks.

General Terms
Image Forgery, Digital Forensics, Region Duplication Forgery

Keywords
Copy –Move Forgery, Copy –Move Attack, Discrete Cosine Transform, Walsh Transform, Orthogonal Transforms, Wavelet Transforms

1. INTRODUCTION
An image is generally accepted as a proof of occurrence of a depicted event. With computer's becoming more prevalent in every field, accepting digital image as an official document has become a common practice [1]. Due to availability of powerful software editing tools such as Photoshop, it has become easier to create, alter and manipulate digital images. If done with proper accuracy these operations are hard to trace. Image tampering or image forgery is applied in various areas such as such as journalism, scientific publications, digital forensic science, multimedia security, surveillance systems etc. A reliable image forgery detection system is needed to evaluate the authenticity and integrity of digital images.

The digital image forgery detection techniques are classified into active and passive approaches [1]. In active approach, the digital image requires pre-processing of image such as watermark embedding or signature generation, which would limit their application in practice. Unlike the watermark and signature-based methods, the passive technology does not need any digital signature to be generated or to embed any watermark in advance. Block matching techniques are employed in passive technology for detecting the forged regions. In block matching, image is first divided into overlapping blocks, followed by feature extraction process. There are three techniques widely used to manipulate digital images. They are:

1. Image Tampering: Image Tampering deals with the manipulation of image to achieve a specific result.
2. Image Splicing: It is a form of photographic manipulation in which there is digital splicing of two or more images into a single composite image.
3. Copy-Move Forgery: In this type of forgery technique, a part of the image is copied and pasted into another part of the same image.

In this paper we have worked on Copy –Move Forgery. In a Copy-Move forgery, a region of the image itself is copied and pasted into another region of the same image. Figure 1 shows an example of Copy –Move forgery. Figure 1 (a) shows original image whereas (b) shows forged image in which truck object is covered with bushes from the same image.

Figure 1: Example of Copy –Move forgery [2] (a) Original Image (b) Forged Image

Because the copied parts come from the same image, its color features, texture, dynamic range, noise components and most other important properties will be compatible with the rest of the image and thus will not be detectable. To make the forgery even harder to detect, one can use the retouch tool like blurring, compression to further mask any traces of the copied-and-moved segments.

This paper is divided into five sections. Section 2 presents literature review, section 3 describes the proposed algorithm, section 4 shows experimental results and section 5 gives conclusion.

2. REVIEW OF LITERATURE
Various methods have been proposed in literature to detect copy –move forgery. The simplest method to detect this forgery is exhaustive search but this method is computationally expensive for medium-sized images. J. Fridrich [2] proposed a method in which image is divided into overlapping blocks and are represented as quantized Discrete Cosine Transform (DCT) coefficients. A.C. Popescu [3]

developed a similar method by applying the principle component analysis (PCA) to yield a reduced dimension representation. Jing Zhang [4] used Discrete Wavelet Transform (DWT) instead of PCA for dimensionality reduction and located copy-move regions by pixel matching. To reduce the ration of false matching blocks Jie Hu [5] developed a method that used the distance of eigen vectors instead of DCT coefficients to fulfill the block. In [6] author propose an wavelet based copy- move forgery detection and applies multi –level 2D DWT. P. Deshpande [7] identifies duplicated regions by matching pixels instead of matching blocks. In [8], author proposed a method which reduced the time complexity for sorting process. The image was decomposed into four sub-bands by applying DWT. Singular Value Decomposition (SVD) was then applied on low – frequency components of these blocks. The SV vector is sorted lexicographically to detect duplicated region. Myna et al. [9] proposed a wavelet transform based approach that detects similar blocks in image by mapping them to log-polar co-ordinates and using phase correlation to find similarity. H. Huang et al. [10] presented a method that detects duplicated regions based on local image statistical features known as Scale Invariant Features Transform (SIFT). These features are invariant to rotation and scaling done before pasting the copied part. In [11], Bayram et al. suggested using Fourier Mellin Transform (FMT) on the image block. In this method, fourier representation of each block is obtained first, then re-sampled the resulting magnitude values into log-polar coordinates.

3. PROPOSED METHOD

In this paper, a wavelet transform is generated from an orthogonal transform and is applied on forged image to detect forgery. Image is first divided into overlapping blocks. The original image with size of M x N will generate (M – B + 1) x (N – B +1) overlapping blocks, where B represents block size. On each block we apply orthogonal wavelet transforms (Wavelet of DCT and Walsh in our case). Further feature vector is created for each block. Feature vector contains following energy signatures extracted from wavelet coefficients [6].

$$\text{Mean} = \frac{1}{n}\sum_{i=1}^{n} x_i \quad (1)$$

$$\text{Norm1} = \sum_{i=1}^{n} |x_i| \quad (2)$$

$$\text{Norm2} = \left(\sum_{i=1}^{n} |x_i|^2\right)^{1/2} \quad (3)$$

$$\text{Standard deviation} = \left(\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2\right)^{1/2} \quad (4)$$

$$\text{Average residual} = \sum_{i=1}^{n} |x_i - \bar{x}| \quad (5)$$

Where, in equations (1) – (5), x is the coefficient, n is the number of coefficients in a block and $\bar{x}$ is mean value.

To compare feature vectors, we first sort all the feature vectors so that vectors with similar values would come together. Each feature vector is compared with each of its following vector until a significant difference is found. Each feature vector corresponds to a block. To find duplicated blocks, we compute a shift vector between two blocks as:

$$s = (dx, dy) = (x - s, y - t) \quad (6)$$

where (x, y) and (s, t) represents the upper left corner pixels of first and second block respectively. If a value of s is found to be above a certain threshold value, then these blocks are considered for matching. Two blocks are matched if all features of that block are same to a particular threshold value. All the matched blocks are then marked with black color to show the output.

3.1 Existing Transforms

This section discusses Discrete Cosine Transform (DCT) and Walsh transform.

3.1.1 Discrete Cosine Transform

This transform converts an image signal into its corresponding frequency components. The DCT transform divides the image into low frequency sub-band, mid frequency sub-band and high frequency sub-band. The high frequency sub-band component can be removed by noise or compression. The low frequency sub-band contains most important visual parts of an image.

3.1.2 Walsh Transform

Unlike the Fourier transform which is based on trigonometric terms, the Walsh transform consists of a series expansion of basis functions whose values are only -1 or 1. These functions can be implemented more efficiently in a digital environment than the exponential basis functions of the Fourier transform [10].

The array formed by Walsh kernel is a symmetric matrix having orthogonal rows and columns. The Walsh transform matrix is obtained from Hadamard Matrix by re-arranging the rows in increasing sign change order.

3.1.3 Generating Wavelet from Orthogonal transform

Wavelets are mathematical tools that can be used to extract information from many different kinds of data, even images. They are needed to analyze data fully. Wavelets have specific properties that make them useful for image processing. Wavelets can be combined using a “shift, multiply and sum” technique called convolution, with portions of unknown signal (data) to extract information from the unknown signal [12]. Wavelets have an advantage over traditional fourier transforms like Short Time Fourier Transform (STFT). Like other transforms, wavelet transforms can be used to transform data and then encode it to achieve effective compression. The wavelet compressions methods are adequate for representing high- frequency components in 2D images.

So far wavelets of only Haar transform have been studied. This paper suggests wavelet generation of orthogonal transforms alias, Walsh transform, and DCT. Also the use of these transform wavelets is proposed and studied for copy – move forgery detection.

Wavelet transform matrix of size P^2 x P^2 can be generated from any orthogonal transform M of size P x P [12]. For example, if we have orthogonal transform matrix of size 9x9, then its corresponding wavelet transform matrix will have size 81x81. i.e. for orthogonal matrix of size P, wavelet transform matrix size will be Q, such that $Q = P^2$. Consider orthogonal transform M of size P x P as shown in Figure 2 & Figure 3[12].

M_{11}	M_{12}	….	$M_{1(P-1)}$	M_{1P}
M_{21}	M_{22}	….	$M_{2(P-1)}$	M_{2P}
. . .	. . .	. . .	. . .	. . .
M_{P1}	M_{P2}	….	$M_{P(P-1)}$	M_{PP}

Figure 2: P x P Orthogonal transform matrix

1st column of M repeated P times — 2nd column of M repeated P times — pth column of M repeated P times

M_{11}	M_{11}	…	M_{11}	M_{12}	M_{12}	…	M_{12}	…	M_{1P}	M_{1P}	….	M_{1P}
M_{21}	M_{22}	…	M_{21}	M_{22}	M_{22}	…	M_{22}	…	M_{2P}	M_{2P}	….	M_{2P}
. .	. .	. .	. .	. .	. .	. .	. .	. .	. .	. .	. .	. .
M_{P1}	M_{P1}	…	M_{P1}	M_{P2}	M_{P2}	…	M_{P2}	…	M_{PP}	M_{PP}	…	M_{PP}
M_{21}	M_{22}	…	M_{2P}	0	0	…	0	..	0	0	..	0
0	0	…	0	M_{21}	M_{22}	…	M_{2P}	…	0	0	..	0
. .	. .	. .				…		…			…	
0	0		0	0	0		0		M_{21}	M_{22}	..	M_{2P}
. .	. .					…		…			..	
M_{P1}	M_{P2}	…	M_{PP}	0	0	..	0	..	0	0	…	0
0	0	..	0	M_{P1}	M_{P2}	…	M_{PP}	…	0	0		0
. .	. .				. .			. .			. .	
0	0	..	0	0	0	..	0	..	M_{P1}	M_{P2}	..	M_{PP}

Figure 3: Q x Q Wavelet transform generated from P x P orthogonal transform ($Q=P^2$)

Figure 3 shows Q x Q wavelet transform matrix generated from P x P orthogonal transform matrix (refer Figure 2) such that $Q = P^2$. To generate the wavelet matrix, every column of the orthogonal transform matrix is repeated P times. Then the second row is translated P times to generate next P rows. Similarly all rows are translated to generate P rows corresponding to each row. Finally the wavelet matrix of the size Q x Q, where $Q = P^2$ is obtained.

4. EXPERIMENTAL RESULTS

To examine the performance of our method, a set of natural images downloaded from internet are considered. The methods are tested on different forged images of size 128 x 128 and in bitmap (.bmp) format. Each natural image is tampered or forged by copying a part of image from the image and pasted to another area of same image. To some images retouching operations is performed after forgery. Retouching operations such as blurring and edge sharpening are used after forgery. Considering block size B =16, DCT wavelet and Walsh wavelet transform of size 16 x 16 is generated from DCT and Walsh orthogonal transforms of size 4 x 4.

Figure 4 shows the original image, tampered image and detected result for ‘tortoise’ image using DCT Wavelet (DCTW) transform.

(a)

(b)

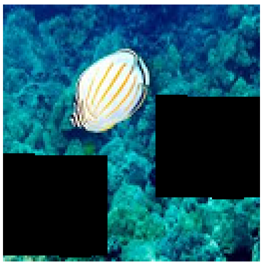
(c)

Figure 4: Output of DCT Wavelet method (a) Original image (b) Forged image (c) Detection Result

Figure 5 shows the original image, tampered image and detected result for ‘fish’ image using Walsh Wavelet (WW) transform.

(a)

(b)



(c)

Figure 5: Output of Walsh Wavelet method (a) Original image (b) Forged image (c) Detection Result

Figure 6 shows the original image, tampered image and detected result for ‘flag’ image using DCT Wavelet (DCTW) transform. Here ‘flag’ image is blurred after forgery using blur tool of Photoshop.

(a)

(b)

(c)

Figure 6: Output of DCT Wavelet method (a) Original image (b) Forged image with blurring operation applied (c) Detection Result

Figure 7 shows the original image, tampered image and detected result for ‘swan’ image using Walsh Wavelet (WW) transform. Here ‘swan’ image is edge sharpened after forgery.

(a)

(b)

(c)

Figure 7: Output of Walsh Wavelet method (a) Original image (b) Forged image with edge sharpening operation applied (c) Detection Result

5. CONCLUSION

In this paper, a wavelet based method to detect copy –move forgery in digital images is proposed. Instead of using basic orthogonal transforms, wavelets of transforms are used. Wavelet transforms for DCT and Walsh transforms are generated respectively using the generation method described in above section. Experimental results show that these transforms are able to detect duplicated regions with more accuracy than using basic orthogonal transforms. This method also detects forged regions even when image is retouched using blurring and edge sharpening operations. However, this method does not detect duplicated regions when copied part in an image is rotated through angles or scaled.

6. REFRENECES

[1] M. Sridevi, C. Mala, S.Sandeep, "Copy-Move Image Forgery Detection In a Parallel Environment", CS & IT-CSCP 2012, pp. 19-29.

[2] Jessica Fridrich, David Soukal, Jan Lukas, "Detection of Copy-Move Forgery in Digital Images", in proceedings of Digital Forensic Research Workshop, August 2003.

[3] A.C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Forgery Regions", Technical Report, TR2004-515, Dept of Computer Science, Dartmouth

[4] Jing Zhang, Zhanlei Feng, Yuting Su, "A new approach for detecting Copy- Move forgery in Digital images", ICCS 2008, pp. 362-366

[5] Jie Hu, Huaxiong Zhang, Qiang Gao, Hai Huang, "An improved lexicographical sort algorithm of Copy –Move Forgery Detection.

[6] Yang Wang, Kaitlyn Gurule, Jacqeline Wise, Jun Zheng, "Wavelet Based Region Duplication Forgery Detection, 2012 Ninth International Conference on Information Technology –New Generations, pp. 30-35

[7] P. Deshpande and P. Kanikar, "Pixel based digital image forgery detection techniques", International Journal of Engineering research and applications, Vol. 2, Issue 3, pp. 539-543 May-June 2012.

[8] G. Li, Q. Wu, D. Tu and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forensics based on DWT and SVD", in proceedings of IEEE international conference on Multimedia and Expo, Beijing ,China, July 2-5 2007, pp. 1750 -1753.

[9] A. N. Myna, M. G. Venkateshmurthy, and C. G. Patil, "Detection of Region Duplication Forgery in Digital Images Using Wavelets and Log-Polar Mapping," in Proceedings of the International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007), Vol. 3, pp. 371-377, 2007.

[10] H . Huang, W. Guo, and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," in Proceedings of IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, pp. 272-276, 2008.

[11] Sevinc Bayram, Taha Sencar, and Nasir Memon, "An efficient and robust method for detecting copy-move forgery," in Proceedings of ICASSP 2009, 2009.

[12] Dr. H.B. Kekre, Dr. Tanuja K. Sarode, Sudeep Thepade, Ms. Sonal Shroff, "Instigation of Orthogonal Wavelet Transforms using Walsh, Cosine, Hartley, Kekre Transforms and their use in Image Compression", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 9, No. 6, 2011, pp. 125-133.