ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

A Review on Copy Move Forgery Techniques

Hitesh Batra [1], Dr.Sanjay Badjate [2]

PG Student, Department of Electronics, S.B. Jain Institute of Technology, Management and Research, Nagpur, India[1]

Vice Principal, S.B. Jain Institute of Technology, Management and Research, Nagpur, India [2]

Abstract: With the presence of image editing software and digital cameras, techniques for digital image tampering are becoming more and more sophisticated and widespread. How to prove the integrity and authenticity of digital images becomes a more and more urgent problem at present, especially in some critical applications, such as court evidence, news broadcast photos, medical images, defence photos, sports pictures etc., in which preserving the exact fidelity of the original image is a legal, moral or technical requirement. Copy-move forgery is one of the widely used tampering techniques where one part of an image is copied to some other part of image in with a view to cover a potentially important feature. In this paper an overview of passive image authentication is presented and the different copy move forgery detection techniques are reviewed.

Keywords: Copy move forgery, Dwt, Dywt, Zernike moment.

I. INTRODUCTION

The trustworthiness of photographs has an essential role in many areas, including: forensic investigation, criminal investigation, surveillance systems, intelligence services, medical imaging, and journalism. The art of making image fakery has a long history. But, in today's digital age, it is possible to very easily change the information represented by an image without leaving any obvious traces of tampering. With the widespread use of powerful digital image editing tools, even people who are not experts in image processing can tamper with an image easily without leaving visible clues.

Thus it poses a very serious social problem as to how much of its content can be believed in, whether it is authentic or tampered, especially as a witness in a courtroom, insurance claims and scientific fraud. Image, as a digital signal is affected by this revolution and its applications are increased in various fields. Specifically, it has found new applications such as being used as evidence in court or news broadcasting. For such usages, the images content must be highly reliable.

On the other hand, the manipulation of digital image is possible, just with a few mouse clicks, using some simple editing software. Usually such tampering is done without leaving any obvious traces; therefore, we need new mechanisms to authenticate the image content. Image authentication techniques can be classified into two categories: active methods and passive methods. Active methods use digital signatures and/or watermark techniques to ensure the integrity of the images. Watermarking techniques requires insertion of some data (called watermark) into image when it was taken. Passive methods do not need the presence of any priority information about the image.

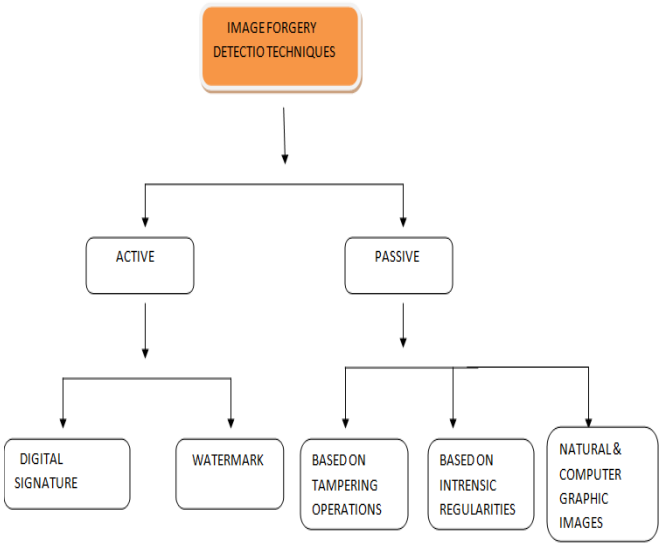
They use some statistical features of the image to determine forgery. Blind passive forgery detection methods are broadly categorized as being (a) visual and (b) statistical. Visual methods are based on visual clues that may not require any hardware or software tools. For example, inconsistencies in images and light deformation on an object within an image.

In contrast, the statistical methods are considered more robust and convincing as they analyze the pixel values of the image. The operations that are performed in blind image forensics have three main aspects:

1. Source identification,
2. Forgery detection and
3. Detection of computer generated images.

Passive-based scheme has been regarded as the new research interest in this field over the last few years. Therefore, verification of content integrity has become increasingly important. Recently, many passive-based schemes for digital image forgery detection have been proposed. Some rely on detecting the traces resulted from image forgery operations such as re-sampling [4], color filter array interpolation [5], camera sensor noise pattern [6], and double JPEG compression [12]. Furthermore, some copy-move or copy-paste detecting methods have been developed [7]-[11]. fig 1 below shows the variety of tampered images.

Majorly the image forgery detection techniques are classified as follows-



DOI 10.17148/IJARCCE.2015.4731

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

II. PROPOSED TECHNIQUES

DYWT

Various previous methods on copy move forgery detection use DWT. However due to its lack of shift invariance, the data analysis is far from optimal. Due to this drawback of DWT, Mallat and Zhong [21] introduced the DyWT, which is shift invariant. In this case, the wavelet transform does not involve down sampling and the number of wavelet coefficients does not shrink between the scales like in DWT. Though the extensively used DWT has been successful in image compression, its performance is far from sublimel in applications such as detection, pattern recognition, or more generally, analysis of data. This is mainly because bi-orthogonal wavelet transform is inadequate of performing translation-invariance property. To overcome the drawbacks of DWT, translation invariant UWT was proposed by Mallat and Zhong [20]. In this case, the number of the wavelet coefficients does not shrink between the scales. This additional information is of great use for the better analysis and understanding of the signal properties.

The general Structure of the proposed algorithm is as follows:

Step I: Image Segmentation: Segment the input image.

Step II: Dywt Transform: Apply Dywt on the input image and get LL and HH sub bands (scale 2).

Step III: Feature Extraction: Using the segmented image, extract the corresponding segments from LL and HH sub bands at scale 2.

Step IV: Feature Analysis: Analyze the pattern of each segment.

Step V:Forgery Detection: Two segments are indicated as tampered if the Euclidean distance between their patterns is less than a threshold *T*.

DWT

Wavelet decomposition of the images are used because of its inherent multi resolution characteristics. The basic idea of using Discrete Wavelet Transform is to reduce the size of the image at each level, e.g., a square image of size 2j ×2j pixels at level L reduces to size 2j/2 × 2j/2 pixels at level L+1. Methods can differ in the type of the wavelet applied. At each level, the image is decomposed into four sub images. The sub images are labelled LL, LH, HL and HH. LL corresponds to the coarse level coefficients or the approximation image. This image is used for further decomposition. LH, HL and HH correspond to the vertical, horizontal and diagonal components of the image respectively.

The general Structure of the proposed algorithm is as follows:

Step I: Image Processing: Read the image given by the user as input. Check the input image if it is not a gray scale image convert it into a gray scale image.

Step II: DWT Transform: Apply Discrete Wavelet Transform b to reduce the size of the image at each level side get reduces to ½ of its original and the image is divided into four sub images, at each level. The sub images are labeled LL, LH, HL and HH [7].LL corresponds the approximate part of the image. This image is used for further processing. After that a *block* of size BXB is slided over the existing image and image is scanned from the upper left corner to the lower right corner. The DWT transform is calculated, For every block, the DWT coefficients are stored as one row in the matrix *A*. The matrix will have $(m-b+1) \times (n-b+1)$ rows and $b \times b$ columns, Where m and n represents number of rows and columns of input image respectively.

Step III: Lexicographically Sorting: lexicographic sorting is performed on the rows of matrix *A*. DWT coefficients for each block are being compared, if two consecutive rows of the sorted matrix *A* are found, the algorithm stores the positions of the identical blocks in a separate list B and increments a shift-vector counter *C*.

Step IV: Normalized shift vector Calculation: Now shift vector is calculated for a suspected pair of blocks, which are at the same vector distance from the corresponding block [8]. The shift vector *v* between the two matching blocks is calculated as$v = (v1, v2) = (x1 – y1, x2 – y2)$\Where (x1, x2) and (y1, y2) are the positions of the two matching blocks. A comparison is done between normalized shift vectors with user-defined threshold T.

Step V: Match block detection: Identification of segments that might have been copied and moved is done by applying same colour on the matching blocks. Thus the threshold value *T* related to the size of the smallest segment can be recognized by the algorithm.

ZERNIKE

Rotation Invariance and robustness to noise made Zernike moments a perfect building block for detecting copy—rotate—move (CRM) manipulations. This section details a specific instance of such detectors. We extract Zernike moments from overlapping blocks of a questioned image and use their magnitudes as feature representation. The detector employs locality sensitive hashing (LSH) [32] for block matching and removes falsely matched block pairs by inspecting phase differences of corresponding Zernike moments.

Copy-move detection algorithm Dwt + Zernike.

Step I: Preprocessing: Conversion of Colour Image into Gray Image. Use of Discrete Wavelet Transform based on dimensioned reduction and extracting .Image resizing into specific scale to reduce the time detection.

Step II: Partitioning: Image is divided into Overlapping Square blocks by Sliding once along the image a window of size b * b from upper left corner right down to the lower right corner

Step III: Feature Extraction: Detection accuracy mainly depends on the ability to map the blocks in a copy move pair to similar features. Wavelet Based: 2D discrete wavelet transform or 2D Dyadic wavelet transform is applied on each block at level 2 and have four sub-bands. Moment Based: Zernike moment are computed on Low frequency sub-band and arranged in a vector. Blocks will be characterized by the magnitude values of the obtained vectors. The method is robust to rotation and noise contamination.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Step IV: Feature Matching and Forgery Detection: Data from Wavelet based, moment based or from both is organized and the similar feature is match using Euclidean distance method. Difference between the coordinates of every matched pairs in case of lexicographic sorting is computed and locates the copy move region.

III. CONCLUSION

In this paper we reviewed forgery detection using three different techniques based on DWT, DYWT, and a combination of Zernike +DYWT.A blind copy-move image forgery detection using UWT and ZM is proposed. By Combining UWT and ZM we make the features translation, scale, and rotation invariant. The proposed method shows its superiority over two other methods by giving a very low false detection rate plus its uniqueness of rotation invariance gives Zernike moment an edge from other methods.

REFERENCES

[1] B.L.Shivakumar, Lt. Dr. S.Santhosh Baboo" Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods "Global Journal of Computer Science and Technology Vol. 10 Issue 7 Ver. 1.0 September 2010

[2] Sarah A. Summers, Sarah C. Wahl "Multimedia Security and Forensics Authentication of Digital Images"http://cs.uccs.edu/~cs525/studentproj/proj52006/sasummer/doc/cs525projsummersWahl.doc

[3] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copymove forgery in digital images," Proceedings of the Digital Forensic Research Workshop. Cleveland OH, USA, 2003.

[4] Bayram, S. et al. 2009. An efficient and robust method for detecting copy-move forgery. *Proc. ICASSP09*, pp. 1053- 1056.

[5] Mahdian, B. and Saic, S. 2007. Detection of copy-move forgery using a method based on blur moment invariants. *Forens . Sci. Int*., vol. 171, no. 2–3, pp. 180–189.

[6] Li, G. et al. 2007. A sorted neighborhood approach detecting duplicated forgeries based on DWT and SVD. *Proc. ICME2007*, pp. 1750-1753.

[7] Chee-Way Chong, P.Raveendran, R.Mukundan. Translation invariants of Zernike moments. PatternRecognition. 2003, 8(36): 1765-1773.

[8] Kim, H.S., Lee, H.K.: Invariant image watermark using Zernike moments. IEEE Trans.Circuits and Systems for Video Technology 13(8), 766-775 (2003).

[9] Mallat S, Zhong S. Characterization of signals from multiscale edges. IEEE Transactions on Pattern Analysis and Machine Intelligence. 1992, 14: 710-32.

[10] Starck Jean-Luc, Fadili Jalal, Murtagh Fionn. The undecimated wavelet decomposition and its reconstruction. IEEE Transactions on Image Processing 2007; 16(2): 297-309.