Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.702 – 708

REVIEW ARTICLE

A Review on Copy-Move Forgery Detection Techniques Based on DCT and DWT

Pameli Mukherjee[1], Saurabh Mitra[2]

[1,2]Dr.C.V.Raman University, Bilaspur, India

[1] Pamelimukherjee89@gmail.com; [2] saurabh.mit1000@gmail.com

Abstract- In today's digital world, authenticity and integrity of any image cannot be taken for granted. Gone are those days when image manipulation was limited to experts only. Digital photography, Photoshop and computer graphics have made image forgery both easier to commit and harder to detect. Amongst various image forgeries known, copy-move forgery stands as a serious threat to the society and image forensic experts. The success of this forgery is due to the fact that copied segment comes from the same image and hence, the properties such as color palette, dynamic range, noise level and texture remains compatible with the entire image, thus, making its detection difficult. Researchers have developed various techniques to counter this kind of attack based on exhaustive search and block matching approach. However, block matching is the most adopted approach due to its speed of operation and cost effectiveness as compared to exhaustive search. In this paper, we review some techniques based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

Keywords- Image Tampering, Image Compression, Copy-Move Forgery, DCT, DWT

I. Introduction

It is very well said that pictures speak louder than words. Researches have also shown that human mind can retain visual images much more easily and long lastingly. When your audience has least time to spare over a long running paragraph, images can do your job at once. It can be easily analyzed that images in the newspapers, magazines, pamplets, advertisements, websites appeal far better than long articles associated with them.

It is always believed that what really occurs, gets captured into the camera. That's why, images have always been taken as a proof of evidence in the court of law, newspapers, journals, medical fields and various other areas. But with rapid advancements in technology, it is possible for a common man to manipulate an image using easily available and low cost image editing tools and software[22].Editing done may be either to improve the quality of the image or to alter the information it conveys. In the former case, the processed image carries the same information as the original but in a more useful way(innocent editing).While in the latter case, the semantic

information conveyed by the image is usually changed by adding or hiding something(malicious editing)[25].Intentional manipulation or alteration done to change the contents of an image is termed as image forgery. The motive behind forgery may be fun-making, harassment, social defamation and political rivalry.

Original Tampered

Figure 1. Copy-Move forgery example

Image tampering is defined as a kind of forgery where some part of the image is added or removed in order to manipulate the information it conveys. Technically, the forgerer changes the pixel values and location depending on the motive, along with some transformations such as rotation, scaling etc. Image tampering comprises three types of forgery viz. cloning(copy-move),splicing and retouching. Cloning is a situation where some part of the image is copied or cloned and pasted on to another specific area of the same image. The sole motive here is to hide some important portion of the image. The situation becomes more cumbersome when some kinds of transformations are applied before pasting the region of interest and hence, these are harder to detect as properties of the copied and moved region remains the same. Second type of tampering includes image splicing which is a process that involves collecting specific regions from different images and assembling them onto a single image. Lastly, retouching involves enhancement of the image by adjusting colors, contrast, noise, sharpness etc.

The techniques used to counter these forgeries come under image tampering detection techniques. These detection techniques may be either classified as active or passive. Active detection approach requires post-processing manipulations of the image after they have been captured by the image capturing device. Active approach includes embedding a digital copy of the image into the image itself, known as self embedding and other one is digital signature, where a compact form of the image is inserted into the host image. However, millions of images that are already on the internet cannot benefit from this approach.

Passive approach does not require prior presence of digital signature or watermark to authenticate the image. This approach takes into account, the statistics of the image in order to detect forgery. Hence, it comes out to be the most useful approach for those images that are already on the web[26].

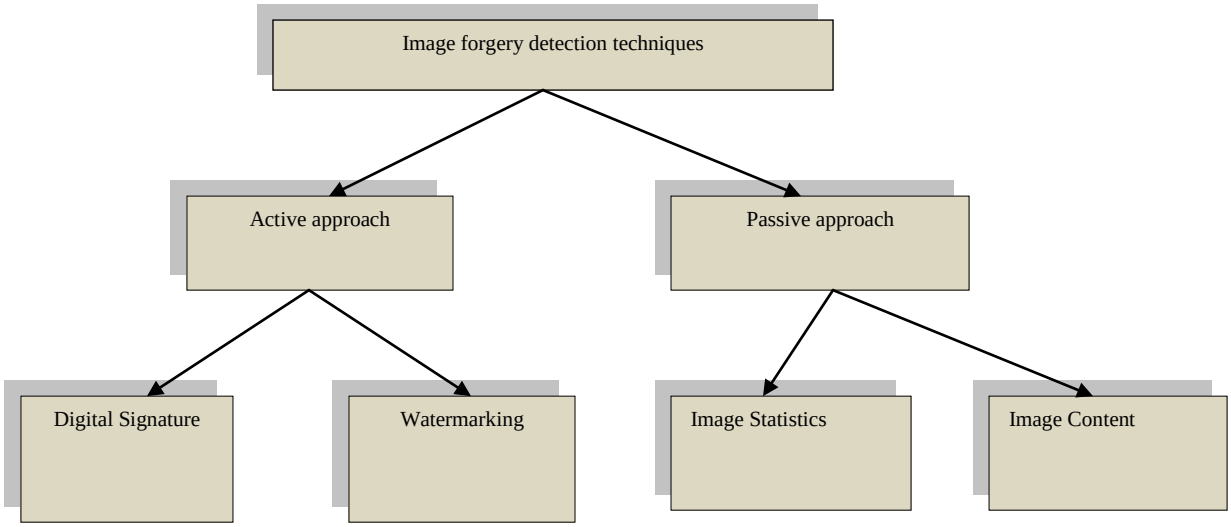

Figure 2. Forgery Detection Techniques Classification

A. .Image compression techniques

1) Discrete Cosine Transform: This transform is used to convert spatial domain image into discrete spatial frequency domain. It was first applied in 1974 for lossy image compression. Efficacy of this transform can be measured from its ability to represent data with few coefficients as possible. It exhibits excellent energy compaction for highly correlated images, parallel implementation capability and requirement of low memory.

One-dimensional DCT sequence of length N is given by

$$C(u)=\alpha(u)\sum_{x=0}^{N-1} f(x)\cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad : \text{for } u=0,1,2,\ldots..,N-1.$$

Inverse transformation is given by

$$f(x)=\sum_{u=0}^{N-1} \alpha(u)c(u)\cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad : \text{for } x=0,1,2\ldots\ldots,N-1.$$

where $$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}}, & u = 0 \\ \sqrt{\frac{2}{N}}, & u \neq 0 \end{cases}$$

2) Discrete Wavelet Transform: Wavelet transform decomposes a signal into a set of basis functions. These basis functions are called wavelets. Wavelets are obtained from a single prototype wavelet y(t) called mother wavelet by dilation and shifting.

$\Psi_{a,b}(t) = \frac{1}{\sqrt{a}} \Psi\left(\frac{t-b}{a}\right)$ Where a is scaling parameter and b is shifting parameter

1-D wavelet transform is given by

$W_f(a,b) = \int_{-\infty}^{\infty} x(t)\Psi(t)dt$

2-D wavelet transform: DWT employs multi-resolution technique for dimensional reduction. Multi-resolution means analyzing different frequencies with different resolutions. At each level, the image is decomposed into four sub-images LL, LH, HL, HH. This image is used for further decomposition. LH, HL, HH correspond to vertical, horizontal and diagonal components respectively. The sub images can be combined to restore the image. In DWT, the most prominent information in the signal appears in high amplitude frequencies. High data compression can be achieved by discarding low amplitude frequency value of the image.

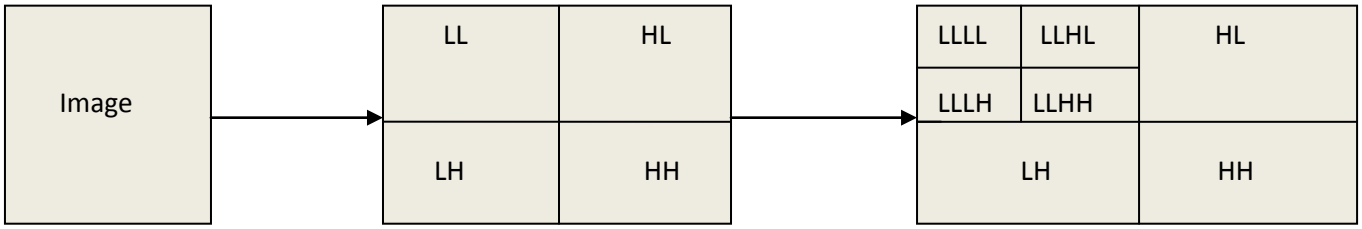

Figure 3 Two-level decomposition of an image using DWT

II. Related Work

Many researches have been done in this direction in the past ten years. The milestone in detecting copy-move forgery based on DCT was set by **Fridrich et al**.[1].They proposed a method for detecting copy move forgery based on exhaustive search and a block matching approach. However, exhaustive search proved to be very complex and hence, block matching based method is adopted. In this method, the image is divided into overlapping blocks for ease. Then, the DCT coefficients are computed for each block followed by lexicographical sort. After sorting, similar blocks are detected and forged regions are found. In this paper, authors performed robust retouching operations in the image. But authors have not performed any other robustness tests.

Popescu et al.[2] proposed a technique for detecting cloned regions in digital images. In this paper, authors applied Principal Component Analysis(PCA) on small fixed size blocks and then computed eigen values and eigen vectors of each block. Lexicographical sorting is applied to sort the matrix into row vector form. Henceforth, duplicated regions are automatically detected using a similarity criterion.

This algorithm is quite efficient and robust in detecting tampered regions. The advantage of this technique is the ability to detect duplicate regions even if the image is compressed or noisy. It is robust to compression upto JPEG quality level 50.

Similarly, **Hu et al**.[6] proposed an improved algorithm based on DCT. For this, forged image is split into blocks of 8x8 pixels. To each block, DCT is applied and the coefficients are quantized using quantization table.DCT coefficients are arranged into a row vector in the zig-zag order to group the similar frequency together. Row vector is then lexicographically sorted and eigen vectors are computed for each vector to detect forged regions.

Like other algorithms, this one is highly robust and accurate and results in less number of false matching rates.

Kumar et al.[10] presented a fast DCT based method for detecting copy move forgery. In this method, the grayscale image is splitted into overlapping square fixed size 16x16 blocks.DCT coefficients are computed over each 16x16 block and arranged into a row vector by sorting the DCT coefficients in zig-zag order. The feature vector is truncated to retain only the low frequency coefficients. All of these vectors are lexicographically sorted into a matrix form. Then, corresponding shift vector is calculated. Blocks with shift value greater than the threshold value are suspected for forgery and marked with red colour in order to distinguish them.

This algorithm is robust against minor scaling and rotation upto 2°.However,the robustness decreases with the decrease in the size of copy moved regions.

Using DWT, Li **et al.**[3] proposed a sorted neighborhood approach for detecting duplicated regions based on Discrete Wavelet Transform(DWT) and Singular Value Decomposition(SVD).Authors used DWT to decompose the image into four sub-images. Since most of the information is present in the lower sub-band only, SVD is used to reduce the dimension in this area. After applying lexicographical sorting, forged area is detected using similarity criterion.

This algorithm is robust to different kinds of copy-move forgeries. At the same time, it is robust to compression up to JPEG quality level 70.

Zhang et al.[4] proposed a scheme based on Discrete Wavelet Transform(DWT).In this paper, authors first applied DWT to the input image to reduce the dimension of the image to be able to work with, easily. They, then, applied phase correlation to compute the spatial offset between the copied region and the pasted one. Pixel based matching algorithm is applied to detect the tampering.

This algorithm has lower computational complexity and is highly robust to post processing methods applied. But the algorithm so defined is highly sensitive to the location of copy-move regions.

Ghorbani et al.[5] proposed Discrete Wavelet Transform-Discrete Cosine Transform(QCD) based copy move forgery detection technique. In this paper, authors used DWT to reduce the dimension of the image. A suitable size block is slided over the low-frequency band of the image to form overlapping blocks. To each block was applied, DCT, to reduce the dimension of the feature vector so extracted. After applying sort, for every pair of adjacent rows in the matrix, they calculated normalized shift vector and counted the number of times, a shift vector appears. A threshold value is set for the count value and the blocks are set to be forged only if the count value exceeds this threshold value.

This algorithm can achieve high degree of accuracy but cannot detect forgeries when the tampered region undergoes post processing like rotation, scaling and heavy compression.

Zimba **et al**.[7] proposed a method based on DWT-PCA to detect copy move forgery. Authors used DWT to reduce the dimensions of the image. Block of suitable size is slided over the low frequency sub band of the image from upper left corner to the bottom right corner of the image, pixel-by-pixel.PCA is applied to each block to reduce the feature vector dimension. Blocks are then lexicographically sorted. They calculated normalized shift vector and then offset frequency. This offset frequency is subjected to morphological processing to give final results.

Their algorithm can detect duplications involving rotation of varying degrees. The only disadvantage is that the duplicated region should be bigger than the block size otherwise, it cannot be detected.

Zimba et al.[8] proposed another approach in relation to their work in the same year. In their approach, input image was decomposed into 4 sub-band images using DWT and the method is proceeded with the low-frequency band. A block of suitable size is slided over the region to result into overlapping blocks. For each block, a characteristic feature vector is computed and stored as a row of matrix which is then radix sorted. For each pair of adjacent rows, normalized shift vector is computed. If the count value of block exceeds the threshold value, forgery is detected.

Authors fabricated more efficient algorithm by using radix sort whose run time complexity is far reduced as compared to lexicographical sort.

Fattah et al.[11] presented a method for detecting copy move forgery based on 2D-DWT.In their approach,2D-DWT is applied to the forged image and approximate DWT coefficients are collected from LL band. This band is splitted containing overlapping and non-overlapping blocks. Candidate blocks are selected from non-overlapping blocks. Overlapping blocks are compared with the selected candidate blocks using Euclidean distance to detect forgery.

This algorithm avoids the huge computational burden in contrast to block matching operation. It provides high level of accuracy in terms of hit rate, miss rate and false detection rate.

III. Conclusion

In this paper, we presented a detailed review on existing copy-move image forgery detection techniques based on Discrete Cosine Transform(DCT) and Discrete Wavelet Transform(DWT).One can analyze that both the techniques have their pros and cons. Success of any of these techniques relies solely on size of copy-moved region, geometrical transformations applied, type of sorting applied, amount of compression introduced and size of block.

REFERENCES

[1]. J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images," in Proceedings of Digital Forensic Research Workshop, pp. 1-10, August 2003.

[2]. A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Technical Report,TR 2004-515,Department of Computer Science,Dartmouth College, 2004.

[3]. G. Li, Q. Wu, D. Tu, and S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD," in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing China, pp. 1750-1753, 2007.

[4]. Jing Zhang,Zhanlei Feng and Yuting Su,"A New Approach For Detecting Copy-Move forgery in digital images",in IEEE International Conference on Communication systems China,pp.362-6,2008.

[5]. M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT(QCD) based copy-move image forgery detection," in 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), pp. 1-4,2011.

[6]. Jie Hu,Huaxiong Zhang,Q.Gao and H.Huang,"An Improved Lexicographical Sort Algorithm of Copy-Move Forgery Detection",in 2nd IEEE International Conference on Networking and Distributed Computing,China,pp.23-27,2011.

[7]. Zimba.M. and Xingming, S. "DWT-PCA (EVD) based copy-move image forgery detection", in International Journal of Digital Content Technology and its Applications,Vol:5,no.1,pp.251-7,2011.

[8]. Zimba.M, and Xingming, S.,"Fast and Robust Image Cloning Detection using Block characteristics of DWT coefficients",in International Journal of Digital Content Technology and its Applications,Vol:5,no.7,pp.359-366,2011.

[9]. Wandji N.,Xingming S. and Kue M.,"Detection of copy-move forgery in digital images based on DCT",2012.

[10]. Mukherjee S.,Kumar S.,and Desai J.,"A Fast DCT based Method for Copy-Move Forgery Detection",in Proceedings of IEEE 2nd International Conference on Image Information Processing",pp.649-654,2013.

[11]. Fattah S.A.,Ullah M.M.I.,Ahmmed I.,and Shahnaz C.,"A Scheme for Copy-Move Forgery Detection in Digital Images Based on 2D-DWT",IEEE Transaction,pp.801-804,2014.

[12]. T. Ng, S. Chang, C. Lin, and Q. Sun, "Passive-Blind Image Forensics," in Multimedia Security Technologies for Digital Rights, chapter 15, pp. 383–412. Academic Press, 2006.

[13]. H. Sencar and N. Memon, "Overview of State-of-the-art in Digital Image Forensics," Algorithms, Architectures and Information Systems Security, pp. 325–344, 2008.

[14]. H. Farid, "A Survey of Image Forgery Detection," Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, Mar. 2009.

[15]. J. He, Z. Lin, L. Wang, and X. Tang, "Detecting Doctored JPEG Images Via DCT Coefficient Analysis," in European Conference on Computer Vision, May 2006, vol. 3, pp. 423–435.

[16]. [1]. F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," in Proceedings of the IEEE, Vol. 87, No. 7, pp. 1079-1107, July 1999.

[17]. P. Meerwald and A. Uhl, "A Survey of Wavelet-Domain Watermarking Algorithms," in Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents, Vol. 4314, No.1 pp. 505-516, 2001.

[18]. A. C. Popescu and H. Farid, "Exposing Digital Forgeries in Color Filter Array Interpolated Images," IEEE Transactions on Signal Processing, Vol. 53, No. 10, pp. 3948–3959, 2005.

[19]. M. K. Johnson and H. Farid, "Exposing Digital Forgeries by Detecting Inconsistencies in Lighting," in Proceedings of ACM Multimedia and Security Workshop, New York, pp.1-9,2005.

[20]. C. T. Hsieh and Y. K. Wu, "Geometric Invariant Semi-fragile Image Watermarking Using Real Symmetric Matrix," WSEAS Transaction on Signal Processing, Vol. 2, No. 5, pp. 612-618, May 2006.

[21]. E. S. Gopi, N. Lakshmanan, T. Gokul, S. KumaraGanesh, and P. R. Shah, "Digital Image Forgery Detection using Artificial Neural Network and Auto Regressive Coefficients," in Proceedings of Canadian Conference on Electrical and Computer Engineering, CCECE 2006, pp.194-197, 2006.

[22]. H. Farid, "Digital Doctoring: How to tell the real from the fake,"Significance, vol. 3, no. 4, pp. 162-166, 2006.

[23]. H. Farid, "Exposing Digital Forgeries in Scientific Images," in Proc. ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006.

[24]. A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Technical Report, TR2004-515, Dartmouth College, Computer Science, 2004.

[25]. Alessandro Piva,"An Overview On Image Forensics," Review Article,Hindawi Publishing Corporation,vol.2013,pp.1-17,2013.

[26]. Abbas Cheddad (2012),"Doctored Image Detection: A brief introduction to Digital Image Forensics",[online]. Available: http://www.inspiremagazine.anasr.org.

