International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

A Comparative Analysis on Copy Move Forgery Detection in Spatial Domain Method Using Lexicographic and Non Lexicographic Techniques

Vidya S. Pujari
Department of Computer Engineering
Vidyalankar Institute of Technology Wadala(E), Mumbai-37
Email: vidyamulki@rediffmail.com

Prof. Mandar Sohani
Department of Computer Engineering
Vidyalankar Institute of Technology Wadala(E), Mumbai-37
Email:mgsohani@rediffmail.com

Abstract **- A digitally altered image, often leaving no visual clues of having been tampered with, can be indistinguishable from an authentic image [1]. Authenticity of digital images plays important role in various fields like medical, legal, criminal, and journalism. Due to rapid advances and availabilities of powerful image processing software, digital images are easy to manipulate and modify for ordinary people. This makes it more and more difficult for a viewer to check the authenticity of a given digital image. In the fields such as forensics, medical imaging, e-commerce, and industrial photography, authenticity and integrity of digital images is essential. This motivates the need for detection tools that are transparent to tampering and can tell whether an image has been tampered just by inspecting the tampered image[3]. Copying parts of an image and pasting in the same image for covering unwanted information or creating a fake image by splicing two or more images are most used techniques in digital image manipulation. These are called copy-move and image-splicing techniques respectively. In this paper we focus on copy-cover image forgery using spatial domain method and do the comparative analysis for lexicographic and non lexicographic techniques.**

Keywords **- Copy Move Forgery, Discrete Cosine Transform, Active and Passive method, Discrete Wavelett Transform, Lexicographic & Non Lexicographic Technique**.

I. INTRODUCTION

During the past decade, powerful computers, high-resolution digital cameras, and sophisticated photo-editing software packages have become affordable and available to a large number of people. As a result, it has become fairly straightforward to create digital forgeries that are hard to distinguish from authentic photographs. These forgeries, if used in the mass media or courts of law, can have an important impact on our society. Unlike conventional film photographs, however, digital images can be easily edited and modified with the aid of today's computer technology. Modification and synthesis of digital images can be easily performed by a novice with available sophisticated image processing software's like Adobe Photoshop, Corel Draw or Gimp. While this has the significant advantage of enjoying the creation of digital works, it has the shortcoming of being maliciously abused in cases where "proof" is required such as in images of medical reports or crime scenes.

II. IMAGE FORGERY DETECTION METHODS

Image Forgery Detection is probably one of the most interesting functions under Digital Image Forgery due to its application which is generally much closer to the public compared to the other two functions. It deals with techniques or algorithm to detect traces of digital image tampering. There are many algorithms or techniques for detecting tampered image. In general, these techniques can be divided into two major groups; Active Method and Passive Method [4].

Active Method requires that certain information is embedded inside an image during the creation or before the image is being disseminated to the public. The information can be used to either detect the source of an image or to detect possible modification of an image. One of the techniques under active method is watermarking. The problem with watermarking is that it requires special hardware or software in order to insert certain information to the image. The user who post images on the internet themselves probably does not bother to use any watermarking software to mark their work, which leads to the inability of using active methods in detecting digital image forgery.

Passive method on the other hand, does not require any pre-'image distribution' information to be inserted into digital image. The method works purely by analyzing binary information of digital image, without any need for external information. However, unlike techniques in active method, techniques in passive methods can be used to detect traces of image forgery but cannot guarantee that an image that passed the test (no detectable traces of image tampering) is authentic or has not been modified in any manner. Techniques in passive method for detecting image forgery can divided into two main category, one that is based on the pixel value of the image (Statistical Method) and one that tries to detect inconsistencies in the image itself based on visual cues (Visual Method). Visual Method is the easiest because sometimes it can be performed without the need for special hardware. One way of detecting traces of image forgery by visual method is to compare lighting information from different parts of an image.

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

(a) (b)

Fig.1. (a) Forged image. Notice the repeating smoke pattern a sign of copy-move attack. (b) The original image.

III. Copy Move Forgery Detection Using Non Lexicographic and LexicographicSpatial Domain Method

Detecting copy-move in an image indulges extensive search of local pattern or region matches [3][4]. One preliminary idea that one gets to detect copy-move forgery is breaking an image spatially in to blocks of size n □ □ n and comparing the blocks for matches. The block size taken should be smaller than the minimum size of assumed tampering. If a part of image is copied and pasted at a different position in to the same image from which it has been derived, it is likely that the forgery introduces correlations between the segment copied and the pasted one. This kind of correlation can be detected by extensive search for similar segments or pixel blocks in the whole image. Let the image to be investigated is of N pixels with a width of Nx pixels and a height of Ny pixels. Let the minimum copy-move size be greater than a block of n □ □ n pixels. The image is split into a number of blocks. This is done by scanning the image at every pixel location with an n □ □ n block and extracting pixel values either column or row wise into rows of a two dimensional array as shown in Figure

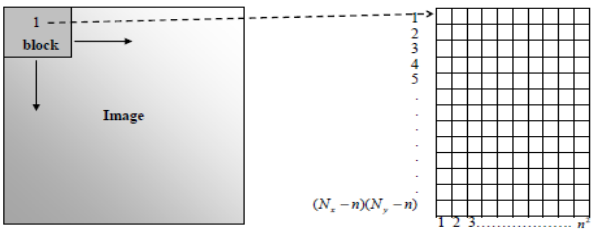


Fig.2. Pixel block scan and array dimensions for the matching algorithm

The index of each pixel block in the array indicates the position of the pixel starting from where the block is extracted from the image. Once the image data is gathered into the array, all the rows are compared with all other rows to find matches. If two rows are identical it is likely to have two identical patterns in image.

One way of reducing the search duration is by sorting the array in lexicographical order and searching from top to bottom of the array for consecutive identical rows. The runtime of the whole matching algorithm lies in the searching of the similar blocks. Lexicographical sorting method ensures least searches among the blocks and hence speeds up the overall performance of the algorithm.Once the elements of the 2D array are sorted in lexicographical order and analyzed, all the rows of the array are compared for matches and their shift values are noted down in a separate list. Since the obtained matches and shift's depend on the number of copy-moves performed and the size of the tampered region. More shifts with equal value indicate tampering rather than random shift values. The resultant shift is used for replacing the tampered pixels indicated by the index of the respective blocks in the 2D array with a color value[4].

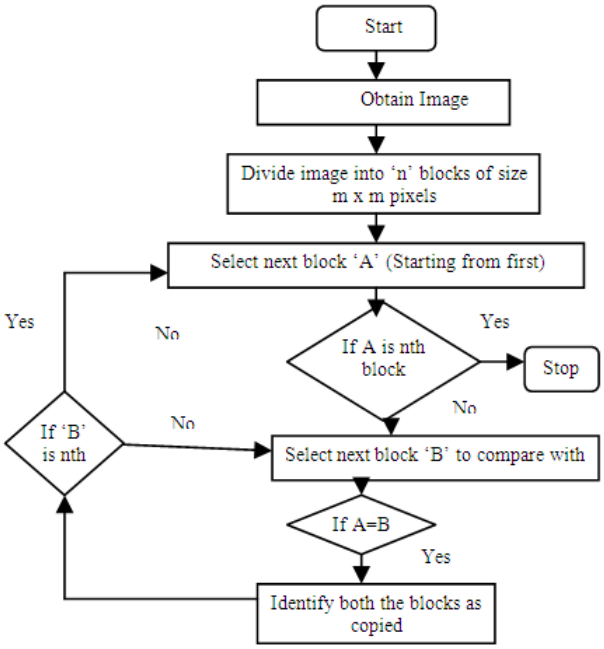


Fig.3. Flowchart of the algorithm for copy-move forgery detection using Non-lexicographic technique

IV. Analysis of Copy Move Forgery Detection Using Frequency Domain Method

Detecting copy-move in an image indulges extensive search of local pattern or region matches. In frequency domain method the image is divided into blocks and to each blocks frequency domain method is applied and then the copy move forgery analysis is performed in frequency domain.Copy-move detection algorithm based on frequency domain method [6] on the kind of analysis performed on the collected data can be classified as

A. Matching quantized dct coefficients (dct):

Instead of spatially analyzing local regions of pixel data, analysis is performed in frequency domain by calculating quantized DCT coefficients for the pixel blocks and searched for matches among the blocks.

B. Matching dwt blocks (dwt):

This methods works by first applying DWT to the input image to yield a reduced dimensional representation .Then the compressed image is divided into overlapping blocks. These blocks are then sorted and duplicated blocks are

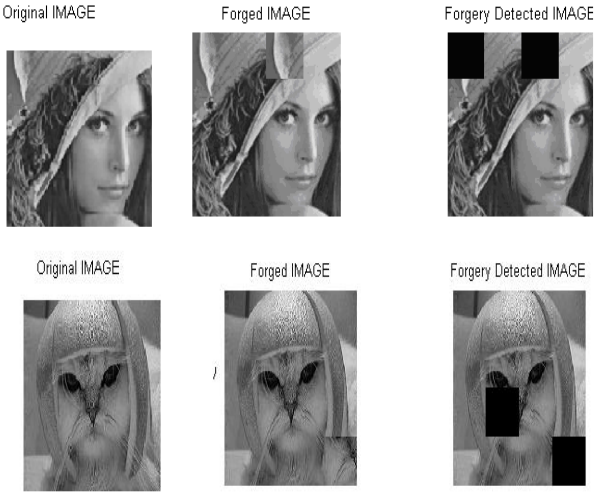
identified using Phase Correlation as similarity criterion. Due to DWT usage, detection is first carried out on lowest level image representation [6][9].

V. Comparision of Spatial Domain and Frequency Domain Method

Spatial Domain	Frequency Domain
In this Image is divided into blocks of size n*n and comparison is done on the actual pixel values	In this Image is divided into blocks of size n*n and comparison is done on the actual pixel values after applying some kind of transformations like PCA, DWT, DST, DCT.
Analysis is performed in Spatial Domain	Analysis is performed in Frequency Domain
Much faster as compared to frequency domain	Much slower as compared to spatial domain method
Less computational involved in the process as works with the actual pixel value.	More computational complexity involved in the process.
Doesn't works for the images where the attacker has made detection more difficult by applying noise and JPEG quality level changes	Works even for the images where the attacker has made detection more difficult by applying noise and JPEG quality level changes
Less robustness to common post processing operations	Nice robustness to common post processing operations

VI. Experimental Results

In our experiments, we have tampered several internet downloaded images by copying and pasting one image block over another, in the same image. Our data set consists of data set has some forged images. The detected results over tampered images is shown below and the image size is 256 x 256



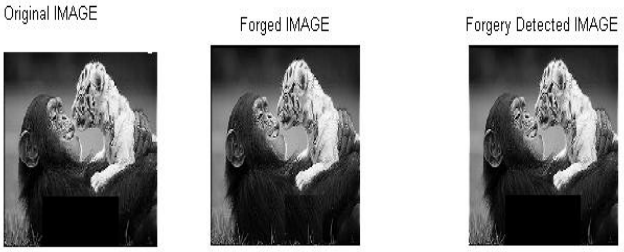


Fig.4. Result Analysis Of copy Move Forgery Detection

Table 1: Results showing the accuracy and comparison time of the algorithm for cat forged image

Algo.	Block size	Block number	Accur Obtained	Time for Comparison(sec)
Non-Lexicographic Sorting	2 x 2	4095	0.3891	106.453
	4 x 4	255	100	0.984
	8 x 8	15	100	0.031
Lexicographic Sorting	2 x 2	4095	0.3891	0.047
	4 x 4	255	100	0.000
	8 x 8	15	100	0.016

VI. Conclusion

Digital image forensics is still a research area at its infancy, there are a lot of things to do. The region-duplication forgery is very common kind of forgery. The development of the forensics of region duplication has told us that today's method must be able to make accurate detection with kinds of disturbance caused by the post processing or other complex middle operations. The proposed spatial domain using lexicographic techniques requires less comparison for checking similarity of blocks as comparison to non lexicographic sorting and hence speeds up the comparison process. Comparison Analysis methods show that spatial domain method using lexicographic sorting is more robust and efficient as compared to spatial domain method using non lexicographic sorting.

References

[1] J Fridrich, D Soukal, And J Lukas. Detection Of Copy-Move Forgery In Digital Images. *Proceedings Of Digital Forensic Research Workshop*, 2003.

[2] Hwei-Jen Lin, Chun-Wei Wang And Yang-Ta Kao. Fast Copy-Move Forgery Detection. *Wseas Transactions On Signal Processing. Issue 5, Volume 5, May 2009.*

[3] Jing Zhang, Zhanlei Feng Yuting Su. A New Approach For Detecting Copy-Move Forgery In Digital Images. *IEEE International Conference On Signal Image Technology And Internet Based Systems 2008*.

[4] Yanping Huang , Weilu , Weisun , Dongyanglong. Improved DCT- Based Detection Of Copy-Move Forgery In Images. *Forensic Science International,Article In Press.*

[5] *Weihai Li And Nenghai Yu.* Rotation Robust Detection Of Copy-Move Forgery. *Proceedings of 2010 IEEE 17th International Conference on Image Processing*

[6] A N Myna, M G Venkateshmurthy, And C G Patil. Detection Of Region Duplication Forgery In Digital Images Using Wavelets And Log-Polar Mapping. *International Conference On*

Computational Intelligence And Multimedia Applications, Sivakasi, Tamil Nadu: IEEE, 2007. 371-377.

[7] Tehseen Shahid, Atif Bin Mansoor.Copy-Move Forgery Detection Algorithm For Digital Images And A New Accuracy Metric. *International Journal Of Recent Trends In Engineering, Vol 2, No. 2, November 2009*

[8] Junwen Wang Guangjie Liu Hongyuan Li Yuewei Dai Zhiquan Wang.Detection Of Image Region Duplication Forgery Using Model With Circle Block. 2009.*International Conference On Multimedia Information Networking And Security.*

[9] Er. Saiqa Khan Er. Arun Kulkarni.An Efficient Method For Detection Of Copy-Move Forgery Using Discrete Wavelet Transform. *(IJCSE) International Journal On Computer Science And Engineering Vol. 02, No. 05, 2010, 1801-1806*

[10] Frank Y. Shih And Yuan Yuan. A Comparison Study On Copy-Cover Image Forgery Detection. *The Open Artificial Intelligence Journal*, 2010, *4*, 49-54

AUTHOR'S PROFILE

Vidya S. Pujari
is working as a lecturer at the department of Information Technology, Vivekanand's Education Institute of Technology, Mumbai. I am also pursuing my post graduation degree (M.E. Computer Engineering) from Vidyalankar's Institute Of Technology, Mumbai. My area of interest include Database Technology, E-commerce, Image Processing, Distributed Systems, Distributed Object Technology, middleware and Enterprise Technology. She has more than 10 years of a teaching experience and have published 5 papers in international and national conference. Email: vidyamulki@rediffmail.com

Prof. Mandar Sohani
is working as a lecturer at department of computer engineering, Vidyalankar's Institute of Technology, Mumbai. He has done B.E. (Electronics Engineering), M.Tech. (Electronics and Telecommunication Engineering). His Area of interest includes Microprocessor, Microcontrollers, Digital Communication, Image Processing. He has more than 11 years of teaching experience and 01 year of industrial experience. He has published many papers in international and national conference. Email: mgsohani@rediffmail.com