Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods

B.L.Shivakumar[1] Lt. Dr. S.Santhosh Baboo[2]

GJCST Computing Classification I 4.1

***Abstract*-As one of the most successful applications of image analysis and understanding, digital image forgery detection has recently received significant attention, especially during the past few years. At least two trend account for this: the first accepting digital image as official document has become a common practice, and the second the availability of low cost technology in which the image could be easily manipulated. Even though there are many systems to detect the digital image forgery, their success is limited by the conditions imposed by many applications. For example, detecting duplicated region that have been rotated in different angles remains largely unsolved problem. In an attempt to assist these efforts, this paper surveys the recent development in the field of Copy-Move digital image forgery detection.**

Keyword-Image forgeries, Digital forensics, Copy-Move forgery detection, block matching

I. INTRODUCTION

From the early days an image has generally been accepted as a proof of occurrence of the depicted event. Computer becoming more prevalent in business and other field, accepting digital image as official document has become a common practice. The availability of low-cost hardware and software tools, makes it easy to create, alter, and manipulated digital images with no obvious traces of having been subjected to any of these operations. As result we are rapidly reaching a situation where one can no longer take the integrity and authenticity of digital images for granted. This trend undermines the credibility of digital images presented as evidence in a court of law, as news items, as part of a medical records or as financial documents since it may no longer be possible to distinguish whether a given digital images is original or a modified version or even a depiction of a real-life occurrences and objects. Digital image forgery is a growing problem in criminal cases and in public course. Currently there are no established methodologies to verify the authenticity and integrity of digital images in an automatic manner. Detecting forgery in digital images is an emerging research field with important implications for ensuring the credibility of digital images [1]. In the recent past large amount of digital image manipulation could be seen in tabloid magazine, fashion Industry, Scientific Journals, Court rooms, main media outlet and photo hoaxes we receive in our email. Digital image forgery detection techniques are classified into active and passive approach [3]. In active approach, the digital image requires some pre-processing such as watermark embedding or signature generation at the time of creating the image, which would limit their application in practice. Moreover, there are millions of digital images in internet without digital signature or watermark. In such scenario active approach could not be used to find the authentication of the image. Unlike the watermark-based and signature-based methods; the passive technology does not need any digital signature generated or watermark embedded in advance [4]. There are three techniques widely used to manipulate digital images [3]. 1) Tampering – tampering is manipulation of an image to achieve a specific result. 2) Splicing (Compositing) - A common form of photographic manipulation in which the digital splicing of two or more images into a single composite 3) Cloning (Copy-Move)

II. COPY-MOVE FORGERY

Copy-Move is a specific type of image manipulation, where a part of the image itself is copied and pasted into another part of the same image (Fig 1).

(a) (b)

Fig 1. An example of copy-move forgery [5]: (a) the original image with three missiles (b) The forged image with four missiles

Copy-Move forgery is performed with the intention to make an object “disappear” from the image by covering it with a small block copied from another part of the same image. Since the copied segments come from the same image, the color palette, noise components, dynamic range and the other properties will be compatible with the rest of the image, thus it is very difficult for a human eye to detect. Sometimes, even it makes harder for technology to detect the forgery, if the image is retouched with the tools that are available.

About-[1]Associate Professor ,Department of Computer Applications. S.N.R. Sons College Coimbatore -641006, India
About-[2]Associate Professor ,PG and Research Dept. of Computer Applications, DG Vaishnav College,Chennai - 600 106, India

III. COPY-MOVE FORGERY DETECTION TECHNIQUES

The simplest way to detect a Copy-Move forgery is to use an exhaustive search. In this approach, the image and its circularly shifted version are overlaid looking for closely matching image block. This approach is simple and effective for small-sized images. However, this method is computational expensive and even impractical for image of medium-sized. In this method for an image size MxN it would take $(MN)^2$ steps, since the comparison and image processing require the order of MN operations for one shift. Another technique for detecting forgery is based on autocorrelation. All Copy-Move forgery introduces a correlation between the original segment and the pasted one. However, this method does not have large computational complexity and often fail to detect forgery.

However, in most other approaches the detected image is divided into overlapping blocks. The idea here is to detect connected blocks that are copied and moved. The copied region would consist many overlapping blocks. The distance between each duplicated block pair would be same since each block are moved with same amount of shift. The next challenge would be extracting features form these blocks, which would yield to very similar or same values for duplicated block. Several authors presented to use different features to represent the image block. These blocks are vectorized and inserted into a matrix and the vectors are lexicographically sorted for later detection. The computational time depends upon factor such as number of blocks, sorting techniques and the number of feature. Suppose an image size is NxN, it is divided into $(N-b+1)^2$ overlapping blocks of size $b \times b$. The blocks are represented as vectors of b^2 dimensions, and sorted in a lexicographical order (**Fig 2**). Vectors corresponding to blocks of similar content would be close to each other in the list, so that identical regions could be easily detected.

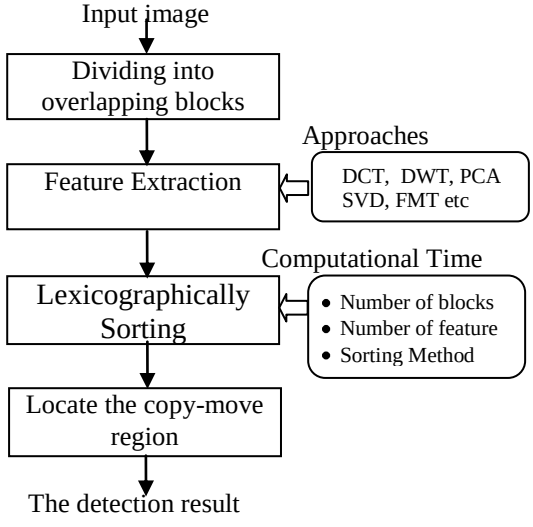
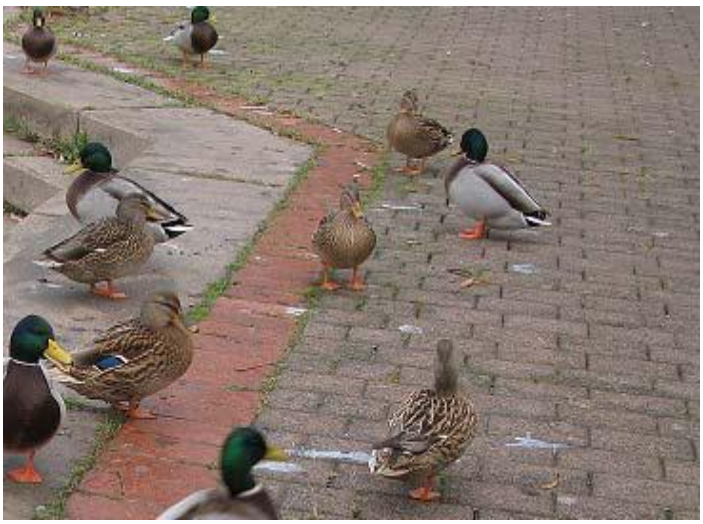


Fig. 2. Configuration of a block Copy-Move Digital Image Forgery Detection System

The image given in Figure 3(a) is the original image and Figure 3(b) is the tampered image by Copy-Move Forgery. As shown in Figure 3(c), the block B1, B2, and block B3 which are copies of blocks A1, A2, and block A3, respectively. Therefore, VA1 =VB1, VA2 =VB2, and VA3 =VB3, where VX denotes the vector corresponding to block X. As shown in sorted list, Figure 3(d), identical vectors are adjacent each other.



(a)

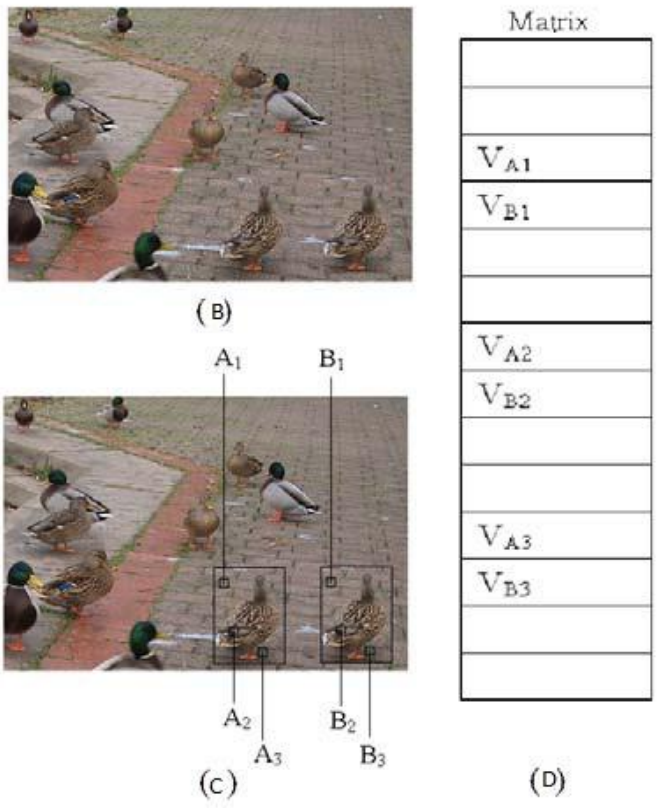


Fig. 3 (a). An original image, (b). Forged image (c) Three pairs of identical blocks are marked by squares, (d). Feature vectors corresponding to the divided blocks are sorting in a list [13]

Over the past 10 years, research has focused on how to make Copy-Move forgery detection system fully automatic. Meanwhile, some significant advances have been made in this field. Nevertheless, many of the finding have important consequences for engineers who design algorithms and system for Copy-Move forgery detection. In the following part of the paper we survey and highlight the summary of research on Copy-Move forgery detection.

A. Region duplication detection: without Scaling and Rotation.

Fridrich et al. [6] suggested the first method for detecting the copy-move forgery detection. In their method, first the image is segmented into overlapping small blocks followed by feature extraction. They employed discrete cosine transform (DCT) coefficients for this purpose. The DCT coefficients of the small blocks were lexicographically sorted to check whether the adjusted blocks are similar or not. In their paper, the method shown was robust to the retouching operations. However, the authors did not employ any other robustness tests.

On the other hand, A.C.Popescu et. al. [7] applied a principle component analysis (PCA) on small fixed-size image to yield a reduced dimension DCT block representation. Each block was represented as 16x16 and the coefficients in each block were vectorized and inserted in a matrix and the corresponding covariance matrix was constructed. The matrix constructed stores floating numbers. By finding the eigenvectors of the covariance matrix, a new linear basis was obtained. Duplicated regions are then detected by lexicographically sorting all of the image blocks. Their method was robust to compression up to JPEG quality level 50 and the time complexity of sorting was $O(32x\ k\ lg\ k)$ time.

Subsequently, G.Li et. al. [8] proposed a method which reduced the time complexity for sorting was reduced to $O(8k\ lg\ k)$. The given image was decomposed into four sub-bands by applying discrete wavelet transform (DWT). The singular value decomposition (SVD) was then applied on these blocks of low-frequency component in wavelet sub-band to yield a reduced dimension representation. The SV vector was lexicographically sorted to detect duplicated region. Their method was robust to compression up to JPEG quality level 70. Later on W. Luo et al. [9] suggested a new method based on the pixel block characteristics. The image was first divided into small overlapped blocks and measured block characteristics vector form each block. Then the possible duplicate region was detected by comparing the similarity of the block. In this approach the time complexity for sorting was further reduced to $O(7k\ lgk)$. Their method was robust to compression up to JPEG quality level 30 and against Gaussian blurring and additive noise with SNR 24 dB.

Myna et al. [10] proposed an approach based on the application of wavelet transform that detects and performed exhaustive search to identify the similar blocks in the image by mapping them to log-polar coordinates and using phase correlation as the similarity criterion.

Recently, Jing Zhang et al. [12] proposed a new approach based on the idea of pixel-matching to locate copy-move regions. In this approach, DWT (Discrete Wavelet Transform) applied to the input image to yield a reduced dimension representation. Then the phase correlation is computed to estimate the spatial offset between the copied region and the pasted region. The task is to locate the Copy-Move region by the idea of pixel-matching, which is shifting the input image according to the spatial offset and calculating the difference between the image and its shifted version. At the end, the MMO (Mathematical Morphological Operations) are used to remove isolated points so as to improve the location. The proposed technique has lower computational complexity and it is reasonably robust to various types of Copy-Move post processing. However, the performance of this method relies on the location of Copy-Move regions.

Ye et. al.[20] described a passive approach to detect digital forgeries by checking the inconsistencies based on JPEG blocking artifacts. There approach consists of three main steps: i) Collection of DCT statistics ii) Analyses of statistics for quantization tables estimation and iii) Assessment of DCT blocks errors with respect to the estimated quantization tables. The experimental result in their paper shows that the blocking artefact measure of JPEG compression version is 97.1. In this paper, the authors failed to mention how to remove the suspicious tampered regions for estimating quantization table. However, Battiato et. al [21], suggests that such techniques are strictly related with the amount of forged blocks in comparison with the total number of blocks.

All the above copy-move methods are most effective for detection when the region is pasted without any change (scaling or rotation) to another location in the image. However, in practice, the duplicated region is often scaled or rotated to better fit it into the surroundings at the target location. Since, scaling or rotation change the pixel values, a direct matching of pixel is unlikely to be more effective for the detection.

B. Region duplication detection: with Scaling and Rotation.

Recently, Bayram et. al [19] suggested a method by applying Fourier Mellin Transform (FMT) on the image block. They first obtained the Fourier transform representation of each block, re-sampled the resulting magnitude values into log-polar coordinates. Then they obtained a vector representation by projecting log-polar values onto 1-D and used these representations as our features. In their paper, the authors showed that their technique was robust to compression up to JPEG quality level 20 and rotation with 10 degree and scaling by 10%.

Hwei-Jen Lin et. al. [13] proposed a method in which each block B of size bxb (=16x16) by a 9-dimensional feature vector. Unlike other techniques, where the feature vector extracted stored floating numbers, this method stored them as integer value. The feature

vectors extracted are then sorted using the radix sort, which makes the detection more efficient without degradation of detection quality. The difference (shift vector) of the positions of every pair of adjacent feature vectors in the sorting list was computed. The accumulated number of each of the shift vectors was then evaluated and the large accumulated number was considered as possible presence of a duplicated region. The feature vectors corresponding to the shift vectors with large accumulated numbers were detected, whose corresponding blocks are then marked to form a tentative detected result. The final result was obtained by performing connected component analysis and medium filtering on the tentative detected result. Even though, the proposed technique reduced the time complexity to $O(9k)$ with help of radix sort, the method failed to detect all copied region of smaller size. According to their experimental results, the scheme performed well when the degree of rotation was 90, 180 and 270 degree. The figure 3 [13] shows duplicated region with and without rotation.

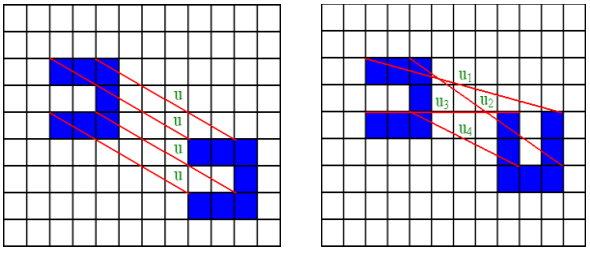


Fig. 3 (a) (b)

a) Duplicated regions form several identical shift vector u.

b) Duplicated region from several (different) shift vector(u_1-u_4) , rotated through 90 degree.

H. Huang et al. [11] presented a method to detect region duplication based on local image statistical features known as scale invariant features transform (SIFT). SIFT descriptors of an image are invariant to changes in illumination, rotation, scaling etc. First the SIFT descriptors of the image is extracted, and descriptors are then matched between each other to seek for any possible forgery in images. Even though this method enables to detect duplication, this scheme still have a limitation on detection performance since it is only possible to extract the keypoints from peculiar points of the image

More challenging situation for detection of copy-move forgery is to detect the duplicated region which is rotated some angle before it is pasted. The method presented by [13] to detect duplicated regions in limited rotation angles. More recently Xunyu Pan et. al[14] suggested a method to detect duplicated regions with continuous rotation regions. As described in [14] the new method was based on the image SIFT features

First the SIFT features are collected from the image, and the image is segmented into non-overlapping examination blocks. The matches of SIFT keypoints in each non-overlapping pixel blocks are computed. After which the potential transform between the original and duplicated regions are estimated and the duplicated regions are identified using correlation map. Even though using SIFT keypoints guarantee geometric invariance and their method enables to detect rotated duplication, these methods still have a limitation on detection performance since it is only possible to extract the keypoints from peculiar points of the image.

Recently, Seung_Jin Ryu et. al[15] suggested a method to detect duplicated region using Zernike moments. The authors proposed to use Zernike moments over other technique since they found it to be superior to the others in terms of their insensitivity to image noise, information content, and ability to provide faithful image representation. A detailed review of relevant studies in Zernike moments is beyond the scope of this paper. For details the readers are referred to the papers [16-18]. In their experiment, 12 different images were used to detect Copy-Move forgery with various manipulations such as rotation etc. In the proposed method the image was divided into MxN overlapped sub-blocks of LxL and calculated the magnitude of Zernike moments to extract vectors of each sub-block. The vectors were then sorted in lexicographically order. Finally, the suspected region is measured by *Precision*, *Recall*, and *F1 –measure* which are often-used measures in the field of information retrieval. The experimental result in their paper show that their system could detect duplicated region rotated some angle before it is pasted, the system is weak against scaling or the other tempering based on affine transform.

IV. Conclusion

As Copy-Move forgeries have become popular, the importance of forgery detection is much increased. Although many Copy-Move Forgery detection techniques have been proposed and have shown significant promise, robust forgery detection is still difficult. There are at least three major challenges: tampered images with compression, tampered images with noise, and tampered images with rotation. In this paper we reviewed several papers to know the recent development in the field of Copy-Move digital image forgery detection. Sophisticated tools and advanced manipulation techniques have made forgery detection a challenging one. Digital image forensic is still a growing area and lot of research needed to be done.

V. References

1) H.T. Sencar, and N.Memon, “Overview of State-of-the Art in Digital image Forensics”, World Scientific Press, 2008
2) H . Farid, “A Survey of image forgery detection”, IEEE Signal Processing Magazine, Vol. pp. 16-25, 2009
3) B.L.Shivakumar and S.Santhosh Baboo, “Digital Image Forgery Detection”, SAJOSPS, Vol. 10(2), pp. 116-119, 2010
4) Lou Weigi, Qu Zhenhua, Pan Feng, and Herang Jiwu, “ Survey of Passive Technology for Digital

Image Forensics", Frontiers of Computer Science in China, Vol. 1(2), pp. 166-179, May 2007

5) Nizza, M., Lyons, P.J.: In an iranian image, a missile too many. In: The Lede, The New York Times News Blog(2008) http://thelede.blogs.nytimes.com/ 2008/07/10/in-an-iranian-image-a-missile-too-many/.
6) Fridrich, D. Soukal, and J. Lukás, "Detection of copy move forgery in digital images," in Proc. Digital Forensic Research Workshop, Aug. 2003.
7) A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Technical Report, TR2004-515, Department of Computer Science, Dartmouth
8) 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, July 2-5, 2007, pp. 1750-1753.
9) W .Luo, J. Huang, and G. Qiu, "Robust Detection of Region Duplication Forgery in Digital Image," in Proceedings of the 18th International Conference on Pattern Recognition, Vol. 4, 2006, pp. 746-749.
10) 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.
11) 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.
12) Jing Zhang, Zhanlei Feng and Yuting Su, "A New Approach for Detecting Copy-Move Forgery in Digital Images", in: IEEE Singapore International Conference on Communication Systems, Guangzhou, China, pp. 362-366, 2008
13) Hwei-Jen Lin, Chun-Wei Wang, Yang-Ta Kao, "Fast Copy-Move Forgery Detection", in WSEAS Transaction on Signal Processing, Vol 5(5), pp. 188-197, May 2009.
14) Xunyu Pan and Siwei Lyu, "Detecting Image Region Duplication Using SIFT Features", in: International Conference on Acoustics, Speech, and Signal Processing, Dallas, TX, 2010
15) Seung-Jin Ryu, Min-Jeong Lee and Heung-Kyu Lee, "Detection of Copy-Rotate-Move Forgery using Zernike Moments", in: 12th International Workshop on Information Hiding, Calgary, Alberta, Candada, 2010
16) Kim, H.S., Lee, H.K., "Invariant image watermark using Zernike moments", IEEE Trans. Circuits and Systems for Video Technology, Vol. 13(8), pp. 766-775, 2003.
17) Khotanzad, A., Hong, Y.H., "Invariant image recognition by Zernike moments",.IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 12(5), pp. 489-497, 1990.
18) Teh, C.H., Chin, R.T, "On image analysis by the methods of moments", IEEE Trans. Pattern Analysis and Machine Intelligence Vol.10(4) , pp. 496–513,1988.
19) Sevinc Bayram, Taha Sencar, and Nasir Memon, "An efficient and robust method for detecting copy-move forgery," in Proceedings of ICASSP 2009, 2009.
20) S.M. Ye, Q.B. Sun, and E.C. Chang, "Detecting digital image forgeries by measuring inconsistencies of blocking artifact", in Proc. IEEE International Conference on Multimedia and Expo 2007, Beijing, China, pp.12-15, July 2007.
21) Sebastiano Battiato AND Giuseppe Messina, "Digital Forgery Estimation into DCT Domain – A Critical Analysis", in Proc of the First ACM workshop on Multimedia in forensics, China, pp. 37-42 , 2009.