State-of-The-Art in Block based Copy Move Forgery Detection

Dr. Indumathi J and Amala S.P

Department of Information Science and Technology,
College of Engineering, Anna University, Chennai, India

Abstract-Digital Images are the reliable means of communicating visual information. It finds a wide range of application in our day-to-day life such as evidence. Throughout our day, what we come across almost all the time are images. In today's sophisticated world of advanced technologies, the reliability of these digital images has been put into question. This is because of the widely available image processing software's that even a novice tampers and creates a synthetic image, counterfeiting both its origin and content. Moreover the technology advent has also led to these forgeries difficult to distinguish from the authentic photographs. It incorporates a skilful tampering of images whereby, deceiving the viewers and avoiding further suspicion. Thus a number of digital image forensic techniques have been developed to verify the authenticity of digital images. This paper gives an idea on the digital image forensics and a survey specially focusing on the Block based copy move forgery detection method.

Keywords- Digital Image Forensics, Image forgery detection, Transform domain robust feature sub-block matching method, Rotation Invariant feature sub-block matching method, Block based copy move forgery detection

I. Introduction

History is puzzled with the remainders of photographic tampering. Ever since Frenchman Nicephore Niepce created the first photograph in 1814, manipulation of photographs also started from, the famous Stalin, Mao, Hitler, Mussolini, and Castro to till date for deceiving the viewers. In Stalin's day, such images required long hours of heavy work. "The Two Ways of Life" a photograph created by Oscar G. Rejland in 1857, one of the first examples of image forgery is said to be an analog composition of 30 images.

Many of the famous photographs in history were the altered ones, for example, the renowned portrait of Abraham Lincoln (circa 1860) was made by merging Senator John Calhoun's body and Abraham Lincoln's head. Today, modern software has made manipulation of photographs easier to carry out and harder to uncover than even before. But the growing technologies also enable new methods of detecting doctored images.

The doctored images lead to counterfeiting, evidence tampering, antique faking, political propaganda, yellow journalism, and defects in scientific research, entertainment and urban myths and much more. Therefore a proper digital image forgery detection approach is required for a reliable visual communication. The organization of this paper is as follows. Section 2 discusses the different aspects of a digital image. The image forgery detection techniques are explained in Section 3. Section 4 gives the advantages and limitations of the copy move forgery detection methods. The final conclusions are given in Section 5.

II. Different Aspects of a Digital Image

A digital image has to be viewed in two different aspects such as:
Is the image real? Or

1) Has it been generated by a computer i.e., Computer graphics
2) Has it been altered by any image processing software.

Thus a digital image forensic technique aims at answering some of the questions [14]. Such as:

- Which imaging device captured this image?
  - Was this image acquired from camera C1 or C2?
  - Was this image originally acquired with camera C as claimed?
  - Was this image a CG or a digital photograph.

- What is the processing history of this image?
  - Is this image an original one or has it been created by splicing other images?
  - Does this image represent a real time situation or has it been tampered with to deceive the viewer?
  - Which part of this image has undergone manipulation and to what extent?
  - What are the consequences of such manipulations?

- Does this image conceal any hidden data?
  - Which algorithm or software has been used to perform the hiding?
  - Is it possible to recover the hidden data?

This paper mainly addresses the questions on the processing history of an image. The inconsistencies or manipulations in the processing of a digital image can be handled by the forgery detection techniques.

III. Image Forgery Detection Techniques

The image forgery detection techniques are based on two types of approaches namely the active approaches and passive approaches. Active approaches constitute watermarking and Digital Signatures. Active approaches need any prior information about the investigated image or its source and moreover removing or inserting watermark itself may lead to distortions in an image. Hence we go for passive approaches. Passive approaches are regarded as a new direction. This area is growing rapidly. Passive approaches do not need any prior information about the investigated image or its source. They mostly, try to analyze each forgery type separately (duplicated image regions, resampling, double JPEG compression, inconsistent noise patterns, etc.) and detect each type separately.

There are different methods for detecting an image forgery such as the Copy-Move forgery detection, Variations in Image features, Inconsistencies in Image features, Lighting inconsistencies, Acquisition inconsistencies, and JPEG inconsistencies. This paper limits its scope to the copy move forgery detection as copy-move operation is the common image tampering method. Here a part of the image is copied and pasted in some other area of the same image with the intent to cover an important image feature.

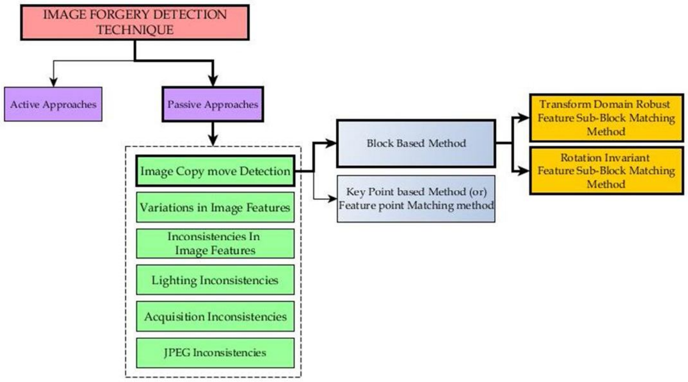
IMAGE FORGERY DETECTION TECHNIQUE
Active Approaches
Passive Approaches
Image Copy move Detection
Variations in Image Features
Inconsistencies In Image Features
Lighting Inconsistencies
Acquisition Inconsistencies
JPEG Inconsistencies
Block Based Method
Key Point based Method (or) Feature point Matching method
Transform Domain Robust Feature Sub-Block Matching Method
Rotation Invariant Feature Sub-Block Matching Method

Figure 1. Taxonomy of Image Forgery Detection Technique.

A. Copy Move Forgery Detection

Copy - Paste (copy-move) operation is a common image tampering method. It is done by copying the contents of a region in the image and pasting it into the same image in another area to conceal the purpose of the content. Copy - paste or copy - move has the advantage of simple operation, subject to image tampering favor. Fridrich [6]. From New York University published the first academic paper for copy - paste operations. From that a number of academic institutions launched an in-depth study on this issue. Depending on the chosen image feature detection, the method is broadly classified into two categories as Block-based methods and Key-point based method. The block based methods are further categorized into Transform domain robust feature sub-block matching method, and Rotation invariant feature sub-block matching method.

The main aim of this paper is to focus on block based copy move forgery detection methods.

1)Transform Domain Robust Feature Sub-Block Matching Method

Jessica Fridrich [6]. proposed a method detecting copy–move forgery using discrete cosine transform of overlapping blocks and their lexicographical representation in. Alin C. Popescu and Hany Farid proposed a method based on representing image blocks using principal components analysis [13]. Aaron Langille and Minglun Gong proposed a method searching for blocks with similar intensity patterns based on a kd-tree [7]. A copy–move forgery detection method based on seven intensity-based characteristics features [10]. was proposed. Wei proposed a multi-level wavelet decomposition of the image block pyramid decomposition based on wavelet coefficients. It has good effect in reflecting the image feature similarity matching. Guohui proposed [8]. duplicated regions detection method based on wavelet transform and singular value decomposition. Some proposed a single SVD block matching method. Brandon Dybala [5]. proposed a cloning detection method based on a filtering operation and nearest neighbor search in. Babak Mahdian and Stanislav Saic [11]. proposed a method for detecting near-duplicated regions based on moment invariants, principal component analysis and kd-tree. Image block geometric invariant moment copy - paste detection algorithm was established by Jiunn-Wen Wang et al. Ardizzone et al., [1]. proposed a number of characteristics, including the edge, Tamura and Gabor by extracting image texture features similar block matching method. In 2011 Yao et al., proposed a method based on the non-negative matrix decomposition tamper detection methods [18]. Through the binary quantization decomposition coefficients and dictionary sorting algorithm complexity compared to the previous methods have improved to some extent.

2)Rotation Invariant Feature Sub-Block Matching Method

Myrna [12]. proposed a method using the idea of log-polar coordinates and wavelet transforms. Wang et al., [16]. Proposed a round feature-based anti-rotation copy and paste tamper detection method. Bayram et al., [2]. Proposed the use of the Fourier-Mellin transform rotation scale invariant feature copy - paste detection method. Li et al., [9]. Proposed an improved rotation scaling invariant feature based on the Fourier-Mellin transform Copy - Paste detection methods. Ryu et al., [15]. Proposed a copy - paste detection method based on Zernike moment rotation invariant features. Zernike transforms the image block and gets a coefficient based on Zernike moments to sort and match. It can also be used for copied - rotation - Paste tamper detection. Bravo-Solorio et al., [3]. Proposed a method where, first the image block is transformed and log-polar domain is found to get a one-dimensional vector in the angular direction. Similar to Solorio, Wu et al., [17]. Proposed a Fourier transform of polar coordinates. This Fourier transform finds the translations problems such as image rotation and zoom through the cross spectrum between the comparison block to determine whether the image block has undergone copy - rotation - paste operations. Christlein et al., [4]. proposed a method to match the estimated rotation after scaling translation parameters.

IV. Advantages and Limitations of the Categories of Copy-move forgery detection methods

A transform domain robust feature sub-block matching method is thus well suited for detection different geometric operations and multiple tampering over the same image and the rotation invariant feature sub-block matching method is good for detecting multiple copy-paste operations. Both the transform domain and rotation invariant methods have high complexity. The former suffers from finding the higher angle rotation of the copied part in an image and the later limits its detection for considerable zoom operations only. The advantages and limitations of the copy move forgery detection methods are tabulated in Table 1.

Table 1 Advantages and Limitations of the Copy-Move Forgery Detection Methods

Method		Advantages	Limitations
Block-based methods	Transform domain robust feature sub-block matching method	• Easy to implement • Soundness of geometric transformation • Multiple tampering positioning can be detected	• Higher angle rotation count can't be found • High complexity
	Rotation invariant feature sub-block matching method	• Copy-paste operation can be accurately detected and located • Multiple tampering can be detected	• Only zoom operations close to original can be detected. • High complexity
Key-point based method		• Low complexity • Higher robustness of scaling and rotation	• Not addressed for highly uniform texture where salient key-points are not recovered • Algorithm very vague

V. Conclusion

We see that there has been a striking demand for image forensics in the recent years since the digital world is flooded with images of suspicious authenticity. Being aware of the forensic techniques helps us to tell wheter an image depicts its original content what it is intended for. Thus a brief survey of the Block based copy move forgery detection method is discussed.

References

1. Ardizzone, E., Bruno, A., & Mazzola, G., "Copy-move forgery detection via texture description," in *Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence*, pp. 59-64. ACM, October 2010.
2. Bayram, S., Sencar, H. T., & Memon, N., "An efficient and robust method for detecting copy-move forgery", in *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009*. IEEE International Conference on, pp. 1053-1056. IEEE, April 2009.
3. Bravo-Solorio, Sergio, and Asoke K. Nandi. "Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling." In *European Signal Processing Conference*, pp. 824-828. 2009.
4. Christlein, Vincent, Christian Riess, and Elli Angelopoulou. "On rotation invariance in copy-move forgery detection." In *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on*, pp. 1-6. IEEE, 2010.

5. Dybala, Brandon, Brian Jennings, and David Letscher. "Detecting filtered cloning in digital images." In *Proceedings of the 9th workshop on Multimedia & security*, pp. 43-50. ACM, 2007.
6. Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukáš. "Detection of copy-move forgery in digital images." In *in Proceedings of Digital Forensic Research Workshop*. 2003.
7. Langille, Aaron, and Minglun Gong. "An efficient match-based duplication detection algorithm." In *Computer and Robot Vision, 2006. The 3rd Canadian Conference on*, pp. 64-64. IEEE, 2006.
8. Li, Guohui, Qiong Wu, Dan Tu, and Shaojie Sun. "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD." In *Multimedia and Expo, 2007 IEEE International Conference on*, pp. 1750-1753. 2007.
9. Li, Weihai, and Nenghai Yu. "Rotation robust detection of copy-move forgery." In *Image Processing (ICIP), 2010 17th IEEE International Conference on*, pp. 2113-2116. IEEE, 2010.
10. Luo, Weiqi, Jiwu Huang, and Guoping Qiu. "Robust detection of region-duplication forgery in digital image." In *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, vol. 4, pp. 746-749. IEEE, 2006.
11. Mahdian, Babak, and Stanislav Saic. "Detection of copy–move forgery using a method based on blur moment invariants." *Forensic science international* 171, no. 2 (2007): 180-189.
12. Myrna, A. N., M. G. Venkateshmurthy, and C. G. Patil. "Detection of region duplication forgery in digital images using wavelets and log-polar mapping." In *Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on*, vol. 3, pp. 371-377. IEEE, 2007.
13. Popescu, Alin C., and Hany Farid. "Exposing digital forgeries by detecting duplicated image regions." *Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515* (2004).
14. Rocha, Anderson, Walter Scheirer, Terrance Boult, and Siome Goldenstein. "Vision of the unseen: Current trends and challenges in digital image and video forensics." *ACM Computing Surveys (CSUR)* 43, no. 4 (2011): 26.
15. Ryu, Seung-Jin, Min-Jeong Lee, and Heung-Kyu Lee. "Detection of copy-rotate-move forgery using zernike moments." In *Information Hiding*, pp. 51-65. Springer Berlin Heidelberg, 2010.
16. Wang, Junwen, Guangjie Liu, Hongyuan Li, Yuewei Dai, and Zhiquan Wang. "Detection of image region duplication forgery using model with circle block." In *Multimedia Information Networking and Security, 2009. MINES'09. International Conference on*, vol. 1, pp. 25-29. IEEE, 2009.
17. Wu, Qiumin, Shuozhong Wang, and Xinpeng Zhang. "Detection of image region-duplication with rotation and scaling tolerance." In *Computational Collective Intelligence. Technologies and Applications*, pp. 100-108. Springer Berlin Heidelberg, 2010.
18. Yao, Heng, Tong Qiao, Zhenjun Tang, Yan Zhao, and Hualing Mao. "Detecting copy-move forgery using non-negative matrix factorization." In *Multimedia Information Networking and Security (MINES), 2011 Third International Conference on*, pp. 591-594. IEEE, 2011.