International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 10, October-2016

A Review: Block-Based Copy-Move Forgery Detection Methods

Malti Puri
Research Scholar, Dept. of CSE
DAVIET
Jalandhar, India

Dr. Vinay Chopra
Assistant Professor, Dept. of CSE
DAVIET
Jalandhar, India

***Abstract*— Digital image forgery has become very common these days. Any non-expert user can create digital forgery using software's which are very easily available and are very easy to use. Image authenticity is a major concern, because images are used in various fields to give illustrate important information. In this paper we survey various block-based methods used for detecting copy-move forgery.**

Keywords*— *CMFD; copy-move forgery; block-based methods; Digital forgery.

I. INTRODUCTION

In the last few years' due to presence of low-cost and high-resolution digital cameras, there is large amount of digital images all over the world. Also with help of very easy to use Photo editing tools, any non-expert can modify image. Any image manipulation can become a forgery, if it changes semantic of original image. [13]. There can be many reasons for a forgery to be occurred by a forger like: To cover objects in an image in order to either produce false proof, to make the image more pleasant for appearance, to hide something in image, to emphasize particular objects etc. There are many ways to categorize the digital image forgery, but main categories of Digital image Forgery are Enhancing, Retouching, Splicing, Morphing and Copy/Move [9]. Following is brief description of different types of digital image forgery:

A. Image Enhancing

Image enhancing involves enhancing an image with the help of Photoshop such as saturation, blur and tone etc. These enhancements don't affect image meaning or appearance. But somehow effects the interpretation of an image [14]. Enhancing involves changing the color of objects, changing time of day in which the image appears to have been taken, changing the weather conditions, Blurring out objects.

B. Image Retouching

It is basically used to reduce certain feature of an image and enhances the image quality to capture the reader's attention. In this method, image editors changes the background, fill some attractive colors, and work with hue saturation for toning [14].

C. Image Splicing

In image splicing different elements from multiple images are pasted into a single image. At last, one image is obtained from content of different images.

D. Image Morphing

Image morphing is defined as a digital technique that gradually transforms one image into another. Transformations are done using smooth transition between two images.

E. Copy-Move

In copy-move forgery one region is copied from an image and pasted onto another region of the same image. Therefore, source and the destination both are same [9, 14]. Copy Move involves copying regions of the original image and pasting into other areas.

II. COPY MOVE FORGERY ATTACK

Copy-Move is a type of forgery in which a part of image is copied and then pasted on to another portion of the same image. The main intention of Copy-Move forgery is to hide some information from the original image. Since the copied area belongs to the same image, the properties of copied area like the color palette, noise components, dynamic range and the other properties too will be compatible with the rest of the image [4, 13]. So, the human eye usually has much more trouble detecting copy-move forgeries. Also forger may have used some sort of retouch or resample tools to the copied area so as it becomes even more difficult to detect copy-moved forgery. Retouching involves compressing the copied area, adding the noise to the copied area etc. and re-sampling may include scaling or rotating the image. An example is shown in fig.2.2. It is a forged image, which is created by modifying fig. 2.1. Fig. 2.2 is created by copying small portion from the same image and then pasted onto another area of same image. Fig. 2.1 is original image and is used to create forgery.

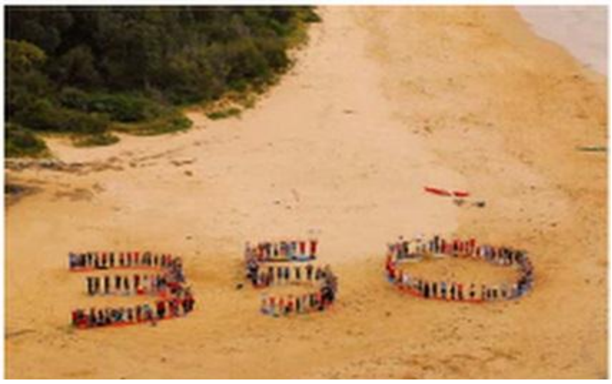

Fig. 2.1 Original Image [13]

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

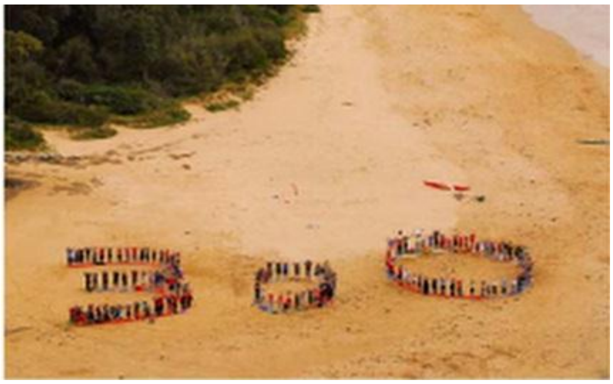

Fig. 2.2 Forged Images [13]

III. NEED FOR DIGITAL IMAGE FORGERY DETECTION

Digital images have become an integral part of almost every area. So, image authenticity and integrity is a major concern [11]. Authenticity of images can't be taken for granted, especially when it comes to legal photographic evidence [10]. Digital images play a very important role in areas like forensic investigation, insurance processing, surveillance systems, intelligence services, medical imaging and journalism. But the basic requirement to believe what we see is that the images should be authentic [3]. Following are some important areas in which integrity and authentication of a digital image is very necessary:

- Medical images are produced in most of the cases as proof for unhealthiness and claim of disease.
- In courtrooms digital images are used as evidence and proofs against various crimes.
- In e- commerce sites images are an essential component when trying to stand out from the crowd and attract customers.

IV. COPY MOVE FORGERY DETECTION METHODS

Digital image forgery detection techniques are mainly classified into two categories: one is active approach and other one is passive approach [2, 15]. See figure 3. Active approach requires a pre-processing step and suggests embedding of watermarks or digital signatures to images [13]. It relies on the presence of a watermark or signature and therefore require knowledge original image. So, it limits their operation. Algorithm/key used to embed the watermark or fingerprint. Any manipulation of the image will impact the watermark and subsequent retrieval of the watermark and examination of its condition will indicate if tampering has occurred. Whereas, in case of passive approach forgery detection, there is no requirement of knowledge of original image. It does not rely of presence of Digital watermark or Digital fingerprint. The passive approach is regarded as evolutionary developments in the area of tamper detection [11].

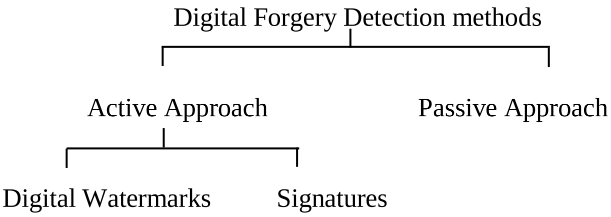

Fig. 4.1 Original Image [10]

Methods for detection of copy move forgery has been categorized into two major categories which are as following:

1. Key Point Based detection.
2. Block Based detection.

In Block based method image is divided into several over lapping blocks. The blocks are compared against each other in order to see which blocks are matched. The regions of the image covered by the matching blocks are the copied and forged regions. In case of Key Point Based method no subdivision of image is done. Rather detection is done on the basis of key points found in the image. These key points are the regions with the high entropy. Both methods differ in only feature extraction rest steps are same

V. BLOCK BASED COPY MOVE FORGERY DETECTION

Block based method splits the image into overlapping blocks and apply a suitable technique to extract features on the basis of which the blocks are compared to determine similarity [1]. Firstly the image is preprocessed i.e. Converted to grayscale. Preprocessing is optional. Then the image is subdivided into overlapping blocks of pixels. For an image size of M × N and a block n size of bxb, the number of overlapped blocks is given by (M-b+1) x (N-b+1). On each of these blocks, a feature vector is extracted. After feature extraction matching is done. Feature vector depends on which feature has been used. Highly similar feature vectors are matched as pairs. Methods that are used for matching are lexicographic ordering on the feature vectors and nearest neighbor determination [9]. Any one from both can be used. The similarity of two features can be determined by different similarity criteria, e.g., the Euclidian distance. There are a number of algorithms that according to the features that are selected for the feature extraction.

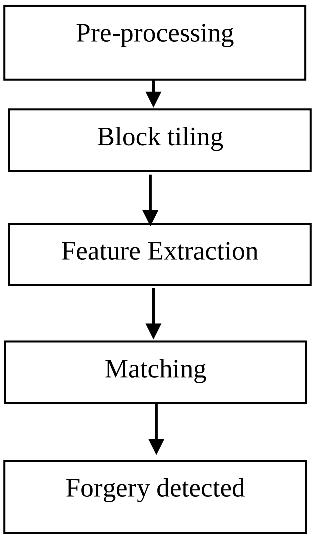

Fig. 5.1 Flowchart of CMFD Detection [13]

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

Following Steps are performed in block-based for Copy Move forgery detection:

A. *Preprocessing*

Preprocessing is the very first step. Also it is optional. Some images required to be pre-processed and some not. Colored image can be converted into grey-scale image to reduce size of image. So, that processing become fast.

B. *Feature Extraction*

In case of Block based method image is firstly divided into several over lapping blocks and this process is known as block tiling. For an image size of M × N and a block n size of bxb, the number of overlapped blocks is given by (M-b+1) x (N-b+1). After block tiling features are extracted from each block. Features like Local binary pattern, discrete cosine transform, discreet wavelet transform Principle Component Analysis etc. are used in block based method.

C. *Matching*

Matching is done to detect the duplicated regions. High similarity between two feature descriptors is interpreted as a cue for a duplicated region. Methods used for matching can be lexicographic sorting, Best-Bin-First search etc. [13].

D. *Forgery detected*

After matching forged regions are detected. Forged regions are marked so that user can see the forged areas.

Jessica Fridrich et.al [2003] investigated the problem of detecting the copy-move forgery and they describes an efficient and reliable copy-move forgery detection method. The method can successfully detect the forged part even when the copied area is enhanced and when the forged image is saved in a lossy format, such as JPEG. They demonstrated performance of the proposed method on several forged images [8].

Babak Mahdian et.al [2006] proposed a method to automatically localize duplicated regions in digital images. The method is based on blur moment invariants. Image is firstly divided into overlapping blocks and blocks are represented using blur invariants. The dimension of the blocks representation is reduced by using the principal component transformation. A k–d tree is used to efficiently perform range queries in multidimensional data for block similarity analysis. The output of the algorithm is a duplicated image regions map. The experimental results show the high ability of the proposed method to detect copy–move forgery in an image even when changes like blur degradation, additional noise, or arbitrary contrast are present in the copied regions [2].

Zhang Ting, et. al [2009] proposed a method based on SVD for detecting copy-move forgery. It works by first extracting singular value SV features, and is then matched to its nearest neighbors in image. Matching is done using searching method of k-d tree. Experimental results shows that the proposed algorithm has low computational complexity and is more robust to post image processing, such as scaling, rotation, noise contamination, Gaussian blurring, lossy JPEG compression etc. [15].

Seung-Jin Ryu et. al [2010] proposed a detection method of copy-move forgery using Zernike moments. The proposed method can detect a forged region even though it is rotated. Also it is robust against additive white Gaussian noise, JPEG compression, and blurring [12].

Er. Saiqa Khan et.al [2010] proposed a technique based on DWT. The technique works by first applying Discrete Wavelet Transform (DWT) to the input image to yield a reduced dimension representation. Then the image is divided into overlapping blocks. These blocks are then sorted. Duplicated blocks are identified using Phase Correlation as similarity criterion. This approach drastically reduces the time needed for the detection process. Experiments prove that the proposed method have nice robustness to common post processing operations. But duplicated regions with rotation through angles and scaled regions cannot be detected [5].

Leida Li et. al [2013] proposed a method based on local binary patterns to detect copy-move forgery. First of all the image is divided into overlapping circular blocks. Then the features of the circular blocks are extracted using local binary patterns (LBP). The feature vectors are then compared and the forged regions can be located by tracking the corresponding blocks. Experimental results shows that this method is robust against JPEG compression, noise contamination, blurring, region rotation and flipping [10].

Guzin Ulutas et.al [2013] proposed a system based on Color Coherence Vector (CCV) to detect copy-move forgery. The vector designates the coherence of the colors in a region. CCV designates coherent pixels in images and use spatial relationship in color information. Forged region accommodates similar CCVs to the original region. Thus, the algorithm can detect forged areas. Experimental results indicate that the method can detect forged regions with high accuracy ratios. Experiments show that the method can detect forged regions even if the image is processed by Gaussian Blurring to hide forgery [7].

Yong-Dal Shin et.al [2016] proposed fast exploration method of copy-move forgery image. Proposed algorithm reduced computational complexity more than conventional algorithms. In this author didn't use 8x8 pixel block exhaustive search method and frequency algorithm to reduce computational complexity. They didn't use exhaustive search method and frequency domain to reduce computational complexity, it uses a half block size in the spatial domain. [14].

M. Buvana Ranjani et.al [2016] proposed an image copy move forgery detection with a new techniques Discrete Cosine Transform Techniques and Inverse Discrete Cosine Transform Techniques by Row and Column Reduction method Initially the original image is divided into matrices, then DCT is applied. Then it is transformed into various blocks with various dimensions. Finally the duplicated image gets sorted out with its threshold value. The method reduces the computational complexity related to time, cost and parallel increase the efficiency of the image. [11].

Beste Ustubioglu et.al [2016] proposed a copy-move forgery detection method that can calculate threshold automatically. Authors uses DCT-phase terms to restrict the range of the feature vector elements. To find similarity between blocks method uses element-by-element equality between the feature vectors instead of Euclidean distance or cross correlation. It utilizes compression history to determine the threshold value for the current test image automatically. Experimental results show that the method can detect the copied regions under different scenarios and gives higher accuracy ratios/lower false negative compared to similar works [3].

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

TABLE I. COMPARISON TABLE

Paper	Method used for feature extraction	Method used for matching	Merits	Demerits
[8]	DCT	Autocorrelation	Can detect the forged part even when the copied area is enhanced or retouched and also when image is in saved in a lossy format.	Uniform areas lead to false matches. Human interpretation is necessary.
[1]	PCA	Row distance	Reduces the dimensionality. Works well even when noise is present.	Doesn't work well for small sized blocks and Signal to noise ratio (SNR) is low.
[10]	LBP	Euclidean distance	Robust against blurring, rotation, noise and flipping.	Difficult to detect forgeries when the region is rotated by general angles.
[2]	Blur moment invariant	k–d tree representation	Can detect forged region with presence of blur and Gaussian noise. Is invariant against contrast changes. Can detect forgery in lossy JPEG format images.	Computational time high.
[15]	SVD	kd-tree, Euclidean distance	Lower computational complexity. Robust against various post image processing.	Is not robust against JPEG compression. It fails to specify that which part is copied and which is pasted.
[5]	DWT	Phase correlation	Reduces the time needed for the detection process and is robust to common post processing operations.	Duplicated regions with rotation and scaling cannot be detected.
[12]	Zernike Moments	Euclidean distance	Robustness against AWGN, JPEG compression and blurring.	Weak against scaling and other forgeries based on Affine transform.
[7]	CCV	Euclidean distance	Can detect forged regions even if the image is processed by Gaussian Blurring.	Can't detect forgeries if postprocessing is done.
[3]	DCT Phase	Element-by-element equality	Robust against post processing operations like JPEG compression, Gaussian Blurring and AWGN. Determines threshold value automatically. It gives higher accuracy ratios and lower false negatives.	------

VI. CONCLUSION

In this era due to presence of low-cost, easy to use and high resolution photo capturing/editing tools it has become very easy to create digital image tampering. Copy-move forgery is one of the digital forgeries. There are basically two categories to detect copy-move forgery i.e. Keypoint-based methods and Block-Based methods. In this paper we survey block-based copy–move forgery detection methods. Each method has its own merits and demerits.

REFERENCES

[1] Alin C Popescu and Hany Farid, “Exposing digital forgeries by detecting duplicated image regions,”Department of Computer Science, Dartmouth College,Tech. Rep. TR2004-515, 2004, pp. 1-11.

[2] Babak Mahdian , Stanislav Saic," Detection of copy–move forgery using a method based on blur moment invariants", Forensic Science International, an international journal dedicated to the applications of medicine and science in the administration of justice, Vol.171 No.2-3 , Sep.2007, pp. 181-189.

[3] Beste Ustubioglu, Guzin Ulutas , Mustafa Ulutas, Vasif V. Nabiyev," A new copy move forgery detection technique with automatic threshold determination”, Elsevier - International Journal of Electronics and Communications Volume 70, Issue 8, August 2016, pp. 1076–1087.

[4] Er. Malti Puri, Dr. Vinay Chopra,” A survey: Copy-Move forgery detection methods”, International journal of computer systems, Volume 3 Issue 8 ,September 2016.

[5] Er. Saiqa Khan, Er. Arun Kulkarni," An Efficient Method for Detection of Copy-Move Forgery Using Discrete Wavelet Transform", International Journal on Computer Science and Engineering, Vol. 02, No. 05, 2010,pp.1801-1806.

[6] Gagandeep Kaur, Dr. Maitreyee Dutta, “Digital Image Forgery: A Survey”, International Journal of Computer Science Research & Technology (IJCSRT), Vol. 1 Issue 6, Nov. 2013, pp.1-7.

[7] Guzin Ulutas, Mustafa Ulutas,"Image forgery detection using Color Coherence Vector", Electronics, Computer and Computation (ICECCO), Nov. 2013, pp. 107 – 110.

[8] Jessica Fridrich, David Soukal and Jan Lukas, "Detection of copy–move forgery in digital images", Proceedings of Digital Forensic Research Workshop, IEEE Computer Society, August 2003, pp. 55–61.

[9] Kusam, Pawanesh Abrol, Devanand,"Digital Tampering Detection Techniques: A Review", BVICAM’s International Journal of Information Technology, Vol. 1 No. 2, 2009, pp.125-132.

[10] Leida Li1, Shushang Li, Hancheng Zhu ,"An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns", Journal of Information Hiding and Multimedia Signal Processing, Volume 4, issue 1, 2013, pp. 46-56.

[11] M. Buvana Ranjani, R. Poovendran, "Image Duplication Copy Move Forgery Detection Using Discrete Cosine Transforms Method", International Journal of Applied Engineering Research, Volume 11, Number 4, 2016, pp. 2671-2674.

[12] Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee"Detection of Copy-Rotate-Move Forgery Using Zernike Moments",Springer Proc. Int. Workshop Information Hiding, 2010, pp. 51–65.

[13] Vincent Christlein, Johannes Jordan “An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Transactions on information forensics and security, 2012, pp. 1-26.

[14] Yong-Dal Shin, "Fast Exploration of Copy-Move Forgery Image" Advanced Science and Technology Letters, Vol.123, 2016, pp.1-5.

[15] Zhang Ting, Wang Rang-ding, "Copy-Move Forgery Detection based on SVD in Digital Image", Image and Signal Processing CISP '09 2nd International Congress, Oct. 2009.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)