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
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 4, April 2018, pg.205 – 212

A REVIEW BLOCK BASED COPY MOVE FORGERY DETECTION TECHNIQUES

Mohamed Ismail[1], Navdeep Kanwal[2]
[1]Computer Engineering, Punjabi University Patiala, India
[1] mohamedismail7725@gmail.com

Abstract:- ***Copy–move forgery the most preceding and predominant forms of intentional qualification doctoring on digital images. That means a of region(s) the two dimensional artefact is (are) copied and pasted onto itself, and then afterwards the suspicious nugget is (are) processed. Main finding on copy moves forgery detection techniques for digital images are merely finding the cloned parts of the image. The few last decades a lot of researches were busy in the area of digital image forensics, whereby the investigation for possible forgeries is solely based on post-processing of images. In this review paper, we will present that was so far found in blocked-based CMD techniques. It reviews findings of the algorithms then evaluates and compare based on their performances related to a set of predefined parameters, this characterization will be used for further evaluation on the performance and efficient of given blocked based cloning detection algorithms under the study.***
The result found after comparing them a user able to select the most optimal forgery detection technique, depending on the user format and type transformation it involves.

I. INTRODUCTION

In today's saturated world digital image become very essential source of evidence for criminal courts as well as media and identity. They are prime carries of information that is used exchange day to day communication of society e.g. Newspapers, social media, websites, television and magazines However due global network a large number of images uploaded to public channels/internet or communication panels are open for intentional and unintentional modification or tempering.

Moreover the wide range availability of the cheap, friendly oriented and more powerful editing software's make the image tempering to put in stake today. Such software makes the modified image undetectable in trivial manner. Manipulations to an image in other word not always are done with unfair intentions.

As we are aware in real life digital image is enhanced with intension of visual quality outlook like X-ray. However, protecting of image integrity and authenticity become chores in due the increase of cyber security.

In few decades there are a many researches done on digital image forgery areas.

Most widely used practises in this domain encompass digital techniques such as *watermarking* and *steganography (active)*. These two techniques enforced only by means of special software's that embedded in the device that processing the image only. Image tampering is defined as a kind of temper where nugget of image is added or removed in order to manipulate the information it conveys.

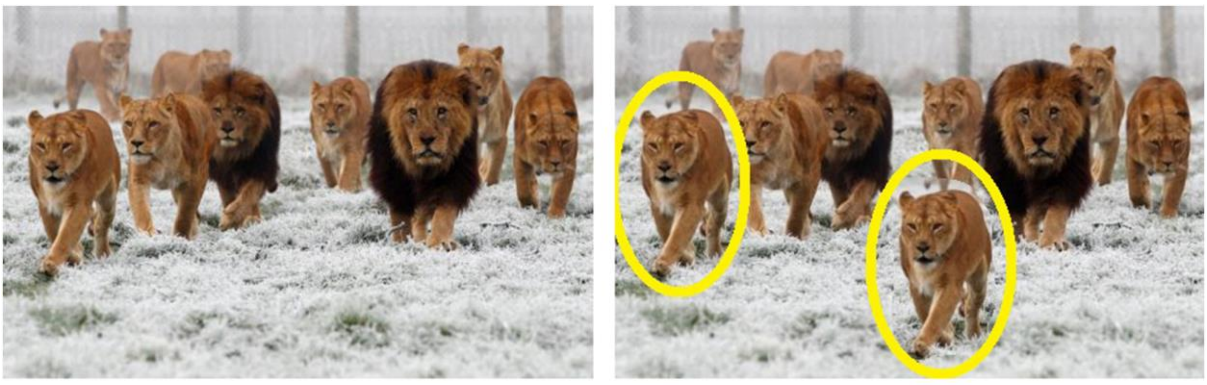
In generally image tempering are classified as cloning, splicing and retouching. Cloning is copy some parts from image and past onto same image to hide some information of the image content. It became trivial means when geometric transformations are applied before pasting the region of interest.

Second type of tampering is splicing which collects and combine parts of different images and assembling them onto a single image and it resemble as different.

Lastly retouching of an image is enhancement purpose like adjusting colours, contrast, noise, sharpness etc.

In digital image can be detected in two ways active and passive in other word active needs prior information while passive not at all.

Passive can be pixel based, camera based, format based, geometric based and physics based. Though we will deals on only the pixel based especially copy-move in block based forgery detection techniques in this review paper.



a *b*

Fig. 1 Example of copy–move forgery

(a) Original image, **(b)** Forged image (duplicated object highlighted)

This cloned image one can see additional lioness in forged image.

Since this kind of image forgery doesn't lead any significant change of image content it doesn't again change the characterises of image like noise, texture colour and so on

Cloned regions can be detected in two techniques that copy-moved forgery image can be detected in digital image such as key point and block based detection here on this paper as we have mentioned will be discussed on block based techniques.

There is a quit difference in case of the cost of computational steps and the number of detected details in block-based detection methods and key point-based methods. Key point-based methods have the advantage of few computational steps (less memory consumption and faster in speed then block-based methods). Such methods, however, cannot produce highly accurate results (detecting only parts of copy-move objects or producing false negatives in flat regions).

II. RELATED WORK

Fridrich et al. [1] these authors firstly suggested a techniques that detecting cloned region of an image. This algorithm divides the suspicion artefact into overlapping blocks a then apply DCT the produced quantized coefficients of each block is recorded; and sorted them lexicographically manner and checked the similarity between adjacent blocks. Hence similar consecutive blocks are considered forged.

Cao et al. [2] proposes region duplication detection algorithm which is based on dividing circular blocks of image and apply with improved DCT this exhibits low computational complexity. The algorithm uses the DCT quantization with quantization table and these circled blocks are again divided into small size, in addition the Euclidian distance between these circular blocks are calculated. This algorithm is good quality in case of blurring and noising image but in poor it's robust.

Kumar et al. [3] come-up fast DCT based method for detecting copy move forgery. Here is how it works as follows suspected image converted into 16x16 overlapping square blocks, then any blocks with shift value that is greater than the threshold then considered as a doctored and marked with red color in order to distinguish them. Its robustness decreases as the size of the cloned region decreases.

Hu et al. [4] divided the image into (8×8) overlapping blocks and computed the DCT coefficients from each block. Feature vector are sorted in zigzag order, and 8 coefficients has been selected, according to frequency, that the array yielded from the quantized coefficients. It is robust in case of

blurring and noise contamination. However, in this work these researchers did not consider more complex transformation (e.g. rotation or scaling).

Popescu and Farid [5] suggested PCA method of copy-move detection.

In this method the image is transformed to grayscale then divides into many parts/blocks represented into vectors. These are organized in lexicographically manner and PCA is used to identify dissimilar blocks in a substitute mode. Moreover, this technique is far efficient for grey scale mostly. It is better for detecting CMF and gives less in false positives. The cost of computational steps and the number of computations required are reduced into O(NtN logN), where Nt stands for dimensionality of the truncated PCA representation and where N is number of pixels. Even though this method has been reduced complexity and highly

Discriminate for large block size, its accuracy is reduced considerably for small block sizes and low JPEG qualities.

Al-Sawadi et al. [8] come up a type of CMFD method which based on Local Binary Pattern and neighbourhood clustering. In this proposed method, the image consists for three components of colour. Each overlapping blocks is used to calculate the LBP histogram. Then after calculating the histogram distance between the blocks and retaining each block-pair that has minimal distances. Then retain each block-pair that the three color components are representing as primary candidates. The candidates are refined by applying the eight-connected neighborhood. Finally the resulted experiment shows improvement in reducing the false positive rates reduction over some recent methods relation. But the performance diminished when rotation and scaling are applied on pasted part.

Davarzani et al. [6] proposed algorithm that detects tempered image based LBP.

This algorithm is differ than the algorithm Al-Sawadi and his colleagues

It detects geometry of the forged region even if it is polluted by noise, blurring, JPEG compression, scaling or rotates in multiples of 90-degrees. Here the image transformed into gray scale then subdivided into overlapping blocks. With multi-resolution Local Binary Pattern features of each block are identified by applying different types of LBP operators. The feature vectors are put together to form feature matrices which their numeral counts which is equivalent the numeral count of LBP operators employed.

The matrices are sorted in lexicographically then k-d tree for determining the matched blocks. Hence Random SAmple Consensus used elimination false matches. However, the method is still have high cost of computational steps and detect in high resolution images, and it cannot detect duplicated regions with arbitrary rotation angles either.

Bayram, et al. [12] conducted a study to detect cloned digital images by using FMT. They choose FMT because robust for likes lossy JPEG compression, blurring, noise, scaling and translation effects applied as post-processing.

At the beginning, the image is splits into several small sized blocks and the Fourier Transform for each block is calculated.

By doing so, they ensured that transform is translation invariant. Then the resulted values are re-sampled, projected and quantized into manner of log polar coordinates to get feature vectors. These feature vectors made rotation invariant to small rotation angles. Then they are matched to find identical feature vectors by using either lexicographic sorting or counting bloom filters. Even a natural image may have several similar blocks. Hence, forging is verified only when there are a certain number of connected blocks within the same distance.

This process reduces false positives making the technique more efficient.

This method could detect forgeries involving blocks with rotations of up to 10 degrees and a scaling of 10%. Their algorithm is also robust to JPEG compression.

Muhammad, et al. [8] proposed a method using un-decimated Dyadic Wavelet Transform, which was chosen because of its property of shifting invariance and thus being more suitable than DWT for analysis of data. Then suspicion image is splits into approximation of both LLI and detail (HH1) sub-bands.

Then both right and left sub-bands are both segmented into an overlapping blocks and their similarity among these blocks are calculated. The main idea is that there should be high similarity of the copied and moved blocks that belong to LL1 sub-band, but low similarities among those from HH1 sub-band because of noise the moved block is full of inconsistency.

Therefore, pairs of blocks are sorted due to high similarity among using LL1 sub-band and high dissimilarity among using HH1 sub-band. Using thresholding, sorted list any pair of matched blocks are obtained with in it. However, these merely detect simple tamper but not scaling of image, its displacement and JPEG compression which is high geometric transformation.

Gomase and Wankhade [14] proposed a block based copy move forgery technique in they used DWT to find out the local intensity of the changes within the image.

Then to eliminate the noise median filtering is applied. For detection process, the image is kept in overlapping blocks of given sizes, store them in a matrix and then sort the matrix. Finally, the matrix is used to indicate the copy-move regions through pixel matching. This method is useful when images are pre-processed, but only shifting of copied regions must in consideration.

Ryu [10**]** introduced Zernike moment method used to localize the doctored region in digital images based on features ZMC blocks. It is robust to compression, noise, and is most important for blurring and rotation invariant. It is needed to accuse the cloned blocks for flat surface of regions.
This method is failed to detect scaled copy-move blocks. The major cons moments based technique is their high computational cost.

Zhong and Xu [11] presented a method that was based on mixed moments.
First, to extraction of the information that has low-frequency from the image Gaussian pyramid transform used then the artefact is divided into overlapping blocks;
Secondly it is lexicographically sorted the block eigenvector using by the moments such as exponenti-fourier and histogram. Thirdly, tampered region was positioned precisely and quickly based to their Euclidean distance and space distance. In shortly Experimental results depicts successfully can detect the forged part of image that is translated, rotated, scaled and mixed operation tamper when the image is changed by brightness variation and contrast adjustment. But the qualitative evaluation, rotation angle and scaling factor are not specified.

Hussain et al. [13] proposed a multi resolution Weber local descriptor system which uses "Weber" law to detect highly textured images with different transformations and shapes of copied regions. Firstly, the colour image into YCbCr mode that stores the colour components in chrominance and luminance factors which can give more information than the human eyes can do.
Then, these components 28 along with WLD are used to get the texture of the image.
The histograms are plotted for each neighbourhood pixel values.
The variations of histograms are how we can find features.
Finally, using SVM classifier, the image is classified as real or fake. Their finds show that 91 % accuracy with multi-resolution using WLD descriptor in the space image chrominance, in addition to giving better discrimination than single resolution, good edge detection, and its being robust to noise change and illumination. Nevertheless, its computation is very complex, and even not possible for images of bigger size.

Quan and Zhang [9] proposed a texture based CMFD scheme in digital images.
The intrinsic dimension estimation techniques is first used to divide the image and then to detect the tempered region of the image with avails same texture.
Lastly founds this algorithm is efficient and robust for retouching and images applied other operations, such as lossy compression, blurring, filtering, etc.

III. CONCLUSION

For last couple of decade's researchers were focused on different types of tempering on digital image, hence this paper will be mentioned for typically of block based the digital image cloned region detection techniques.

This will indicate every technique has its own cons and pros but to evaluate performance of selected techniques based on the set of parameters like size of cloned region, type of transformation and compression ratio and so on that techniques solved. Therefore, none of technique has robust detection way of cloned region.

REFERENCES

1. Fridrich AJ, Soukal BD, Lukáš AJ.(2003) **Detection of copy-move forgery in digital images**. In: in Proceedings of Digital Forensic Research Workshop. Cite seer;
2. Cao G, Zhao Y, Ni R, Li X.(2014) **Contrast enhancement-based forensics in digital images**. Inf Forensics Secure IEEE Trans On.; 9(3):515–25.
3. Bayram S, Sencar HT, Memon N.(2009) **An efficient and robust method for detecting copy-move forgery**. In: Acoustics, Speech and Signal Processing, ICASSP 2009 IEEE International Conference on. IEEE; 2009. p. 1053–6.
4. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, and G. Serra,(2013) "**Copy-move forgery detection and localization by means of robust clustering with J-Linkage**," *Signal Processing: Image Communication*, Vol. 28, No. 6, PP. 659–669, Jul..
5. Popescu A**.(** 2004) **Exposing digital forgeries by detecting duplicated image regions**. Technical Report, TR2004-515, Department of Computer Science, Dartmouth College, Hanover, New Hampshire; USA 2004.
6. Davarzani R, Yaghmaie K, Mozaffari S, Tapak M., (2013), **Copy-Move Forgery Detection Using Multiresolution Local Binary Patterns**. Forensic Science International, vol. 231, issue: 1–3, pp.61–72.
7. Bayram, S. Sencar, H. Memon, N. (2008), **A Survey Of Copy-Move Forgery Detection Techniques**, in Proceedings of the IEEE Western New York Image Processing Workshop, IEEE, pp. 538–542
8. Al-Sawadi, M. Mohammad, G. Hussain, M. Bebis, G. (2013), **Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering**, Modelling Symposium (EMS), 2013 European, (20-22 Nov. 2013), Manchester, pp. 249– 254
9. Quan, X. and Zhang, H. (2012), **Copy-Move Forgery Detection in Digital Images Based on Local Dimension Estimation**, in Proceedings of the International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec '12), pp. 180–185.

10. yu SJ., Lee MJ., Lee HK. (2010) **Detection of Copy-Rotate-Move Forgery Using Zernike Moments.** In: Böhme R., Fong P.W.L., Safavi-Naini R. (eds) Information Hiding. IH 2010. Lecture Notes in Computer Science, vol 6387. Springer, Berlin, Heidelberg
11. Y. Wo, K. Yang, G. Han, H. Chen, and W. Wu,(Feb. 2017) "**Copy–move forgery detection based on multi-radius PCET,"** *IET Image Processing*, Vol. 11, No. 2, PP. 99–108,.
12. Hussain, M. Muhammad, G. Saleh, S. Mirza, A. Bebis, G. (2012), **Copy-Move Image Forgery Detection Using Multi-resolution Weber Descriptors**, in Proceedings of the 8th International Conference on Signal Image Technology and Internet Based Systems (SITIS '12), pp. 395–401
13. Hsu, H. and Wang, M. (2012), **Detection Of Copy-Move Forgery Image Using Gabor Descriptor**, in Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification (ASID '12), IEEE, August 2012, pp.
14. Gomase, P. and Wankhade, N. (2014), **Advanced Digital Image Forgery Detection: A Review**, International Conference on Advances in Engineering and Technology, (ICAET).

