A Review of Copy-Move Image Forgery Detection Techniques

Kanagavalli.N[1], Latha.L[2]
[1, 2] Department of CSE
[1, 2] Kumaraguru College of technology

Abstract- *Digital images are in used broadly in current years and for many purposes. The information will be shared throughout newspapers, magazines, internet, or scientific journals. It is used as a strong evidence beside many crimes and as proof used for many purposes. With the appearance of means of image processing and editing tools, creating or transform images has become simple and available. There are many types of image forgery, one of the most important and prominent type is called copy-move forgery in which a part of the image is copied and pasted into the same image with the aim of hiding something important or showing a false scene. This paper surveys many different types of digital image forgeries and forgery detection methods. The survey has been prepared on existing techniques for tampered image.*

Keywords- Digital image, Copy move forgery, tampering detection, passive approach.

I. INTRODUCTION

In recent years, image is manipulated by adding or removing some elements from the image which results in a high number of image forgeries. Different types of software are available for many applications in image processing. Such software can use to change or modify the image these modifications cannot be detected by human eyes. Therefore, verification of image originality has become a challenging task. An image can be manipulated by many techniques such as blurring, scaling, resampling, filtering, rotation, cropping, etc. Image forgery detection technique is need in many fields for preventing forgery. The verification of image originality is required in many applications such as scientific, military, media, glamour, forensic,etc.

Digital image forgery detection can be classified into two different groups. These are active methods and passive methods. The active approach consists of two parts watermarking and steganography. At the time of image acquisition these are implemented. A special hardware implementation like digital signature or coding the image into different form is needed to mark the authentication of the digital image. The watermarking method is used to hide a mark or a message in a picture in order to protect its copyright at the time of image acquisition and to check the authenticity of message is extracted from the image and verified with the original watermarks. Hiding the important message so that it is not misused by any third party is called steganography.

The passive approach does not require any prior information about the image and it is dependent on the traces left on the image by different processing steps during image manipulation. With the help of different image forgery detection techniques the forged area, location and the amount of forgery can be detected. It includes copy move forgery detection and image splicing and they also help to detect the operations that occur, like rotation, scaling, blurring etc.

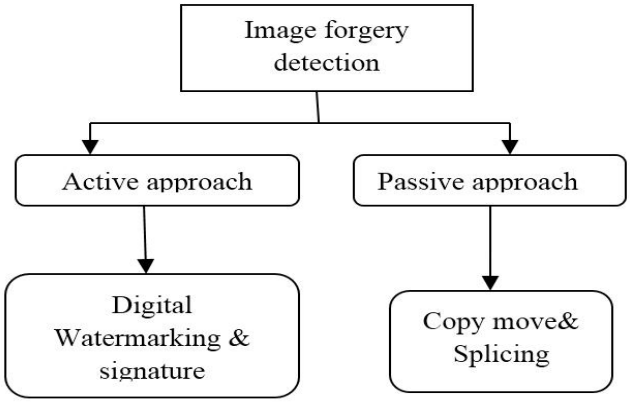

Figure 1. Classification of image forgery

TYPES OF IMAGE FORGERY

A. Copy-Move (Cloning)

Copy-move forgery, also known as Cloning when only one image is considered for the forging process, is more or less similar to image splicing in view of the fact that both techniques modify a certain image region with another image. One region is copied from an image and pasted onto another region of the same image. However, instead of using an external image as a source, copy-move forgery uses portions of the original base image as a source which means that the same image is both the source and the destination of the modified image.

Figure 2. A. Tampered image B. Original image

B. Image Splicing

Different elements from multiple images are sticked together in a single image to convey an idea that doesn't reflect reality. Such splicing can usually be detected by searching the splicing boundary, or the effect of splicing on image statistics, or by considering the directions of the light incident on the image surfaces. A sample of image splicing is shown in Figure 3.

Figure 3. A. Spliced image B. Original images

II. LITERATURE SURVEY

Many techniques have been presented for copy move image forgery detection. The main aim is to classify the same regions in copy move forgery detection but the main issue is how to define similar.

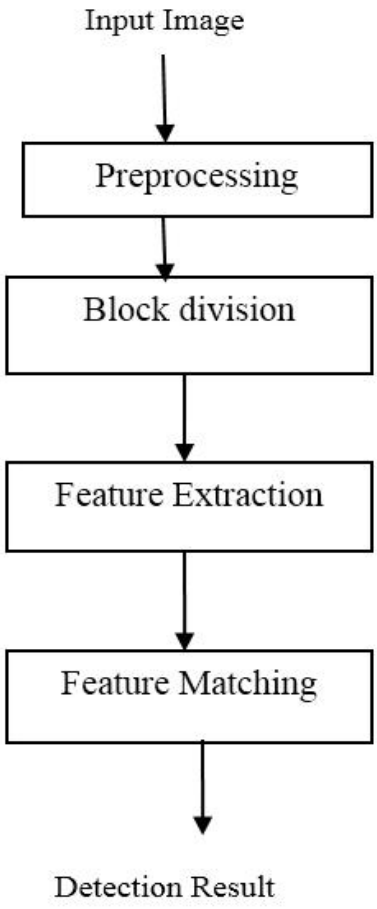

Figure 4. Flow chart

In figure 4, the flow diagram of image forgery detection is explained. At first stage in block based copy move forgery detection techniques, an image may be pre-processed e.g. conversion from color to grayscale image. Then, the preprocessed image is subdivided into overlapping blocks of size B × B. From each of the blocks, a unique representation as feature vectors is obtained. Then, for matching process these feature vectors may be arranged using sorting techniques such as lexicographic sorting, nearest neighbor etc. and some kind of distance measure is used between neighboring feature vectors such as Euclidean Distance. And lastly some morphological operation is applied so that it detects the forged region.

Fredrich, et al[1], proposed a method to detect copy-move forgery. Discrete Cosine Transform (DCT) of the image blocks was used and their lexicographical sorting was considered to avoid the computational burden. Once sorted, the adjacent identical pair of blocks is considered to be copy-moved blocks. A drawback of this method is that it cannot detect small duplicate regions.

Cao et al. [2], present region duplication detection algorithm which depends on improved DCT and exhibits low computational complexity. The profound difference between this method and the other DCT-based methods is that here the quantized block is characterized by a circle block. The circle block is then divided into a fixed number of parts, for which the feature vectors are calculated. Euclidean distance between adjacent pairs is calculated after lexicographic sorting of vectors. The actual distance between the similar vectors is also considered before the final call on duplication is made. This method is capable of identifying multiple region duplications and is also robust against blurring and additive noise but it has poor performance with poor image quality. It is not robust to geometrical operation either.

Zhao and Guo [3], proposed a robust method to detect copy-move forgery based on DCT and SVD. The image is divided into fixed-size overlapping blocks and 2D-DCT is applied to each block. The DCT coefficients are then quantized to obtain a more robust representation of each block followed by dividing these quantized blocks into non overlapping sub-blocks. SVD is applied to each sub-block. Afterwards, features are extracted to reduce each block dimension using its largest singular value. Finally, feature vectors are lexicographically sorted, and the duplicated image blocks are matched by predefined shift frequency threshold. Results showed that the proposed system can spot copy-move forgery even when an image was distorted by Gaussian blurring; Additive White Gaussian Noise (AWGN), JPEG compression or any other related mixed operations.

Popescu and Farid [4], suggested a method using Principal Component Analysis (PCA). In this method the image is transformed into grayscale and separated into many parts represented into vectors. These parts or blocks are organized lexicographically and PCA is used to represent the dissimilar blocks in a substitute mode. It is proficient for detecting even minor variations resulting from noise or wasted compression. Moreover, this technique is far efficient for grey scale images. It is better for detecting copy-move forgeries and gives less number of false positives. Although this method has reduced complexity and is highly discriminative for large block size, its accuracy is reduced considerably for small block sizes and low JPEG qualities.

Al-Sawadi et al[5], presented a copy-move image forgery detection method based on Local Binary Pattern (LBP) and neighborhood clustering. In the proposed method, an image is first decomposed into three color components. LBP histograms are then calculated from the overlapping blocks of each component. The histogram distance between the blocks is calculated and the block-pairs having the minimal distance are retained. If the retained block-pairs are present in all the three color components, they are selected as primary candidates. Eight-connected neighborhood clustering is then applied to refine the candidates. Experimental results show improvement in reducing the false positive rates over some recent related methods. The performance of the methods degrades when the pasted parts undergo both rotation and scaling.

Davarzani et al[6], proposed a tampering detection method based on LBP. This algorithm can detect copied regions even if the geometry of the forged region is further polluted by noise, blurring, JPEG compression, scaling or rotation in multiples of 90-degree. In this algorithm the image is translated into gray scale and is then subdivided into overlapping blocks. Multi-resolution Local Binary Pattern (MLBP) features are identified for each block by applying different types of LBP operators. The feature vectors are put together to form feature matrices which the number is equal to the number of LBP operators employed. Feature matrices are lexicographically sorted and k-d tree method is used for determining the matching blocks. RANdom SAmple Consensus (RANSAC) algorithm is then used to eliminate false matches. However, the method is still time consuming for forgery detection in high resolution images, and it cannot detect duplicated regions with arbitrary rotation angles either.

Bayram, et al [7], conducted a study to detect copy-move forgery by using Fourier-Mellin Transform (FMT). They choose FMT because it is robust to lossY JPEG compression, blurring, noise, scaling and translation effects applied as post-processing. At the beginning, the image is divided into several small sized blocks and the Fourier Transform of each block is calculated. By doing so, they ensured that transform is translation invariant. Then the resulting magnitude values are re-sampled, projected and quantized into log polar coordinates to get feature vectors. These feature vectors made rotation invariant to small rotation angles. Then they are matched to find similar 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.

Shao et al[8], proposed an algorithm which is computationally a complex copy - move forgery detection algorithm. These algorithm dependents on circular window expansion and phase correlation. The image is scanned by a circular window which is then expanded into a normalized

rectangular block using bi-linear interpolation. Discrete Fourier Transform (DFT) is calculated for these expanded blocks to obtain the phase correlation matrix. Enhanced peak values reflect the similarity in regions. A band limitation procedure is applied to the DFT in order to remove the high frequency components as they do not make any constructive contribution towards the calculation of peak values. This method also identifies copied-rotated - moved regions in the image. This method proves to be accurate in forgery detection even after the forged region has undergone rotation, blurring, JPEG compression, and variations in luminance. The drawbacks of this method are represented in the fact that it is not computationally fast and is also not scale invariant.

Hussain et al[9], proposed a multi resolution Weber local descriptor (WLD) system which uses "Weber" law to detect highly textured images with different types of transformations and shapes of copied regions. Firstly, the colored image is changed into YCbCr color mode that stores the color components in chrominance and luminance factors which can give more information than the human eyes can do. Then, these components along with WLD are used to get the texture of the image. The histograms are plotted depending upon neighboring pixel values. Those variations of histograms are connected and plotted to get the features. Finally, using the support vector machine (SVM) classifier, the image is classified as real or fake. Experimental results show that the accuracy rate of this method can reach up to 91 % with multi-resolution WLD descriptor on the chrominance space of the images, in addition to giving better discrimination than single resolution, better edge detection, and its being robust to noise change and illumination. Nevertheless, its computation is very complex, and even impossible for images of bigger size.

Jing and Shao[10], proposed a copy-move forgery detecting method based on local invariant feature matching. This method locates copied and pasted regions by matching feature points. It detects feature points and extracts local features using SIFT algorithm. Matching these features based on Best-Bin-First and k-d tree method. The computational complexity of the proposed method is similar to the existing block-matching methods, but it has better locating accuracy. Experiments show that this method cannot only detect copy-move forgery, but it also detects copy regions with geometrical deformation and some post-operations such as JPEG compression and Gaussian blurring.

Amerini et al[11], employed a Scale Invariant Feature Transform (SIFT) for feature extraction, combined with localization based on the J-Linkage algorithm for detecting tampering. SIFT features are extracted for the image. Afterwards the feature vectors are matched using g2NN algorithm. The Coordinates of the same vectors are considered as candidates for clustering, which are performed by J-linkage algorithm. The result of clustering reveals the copied regions. Because the technique adopts SIFT features, it is able to detecting duplicates involving scaling and rotation. This technique is doing well in detecting several duplications and is also capable of localize tampered parts with a high degree of precision.

Hsu, Lee and Chen[12], presented a copy-move forgery detection scheme using histogram of oriented Gabor magnitude(HGOM). After image preprocessing they have divided the image into fixed size blocks. Then apply Gabor filter and then lexicographical sorting of features is done so that similar features from different blocks are found so that it reduces the matching time, and lastly post processing is done. Multiple copy-move forgery can be detected with the help of this algorithm and also it is robust against attacks like JPEG compression, brightness adjustment, blurring and image rotation, with low computational complexity with the help of two evaluation criteria that is correct detection ratio(CDR) and false detection ratio(FDR).

Ardizzone, Bruno and Mazzola[13], presented a hybrid approach that is matching between triangles which compares triangles instead of single points or blocks. Triangles are matched based on local feature vectors, shapes, and content. High numbers of smaller triangles are present so that the probability to find the matches outside the copied areas is high resulting in less precision, the copy-pasted area that is detected is small and so recall rate decreases. The proposed approach performs good in simple scene and performs worst in complex scene.

III. COMPARATIVE ANALYSIS

Table 1 The queuing parameters and the time and source functions are given as follows.

Sno	Techniques	Parameters	Merits	Demerits
1	Discrete Cosine Transform DCT[2]	Euclidean distance	Detects copy move Region, as well as Blurring and noisy images are detected	It cannot detect small duplicate regions.
2	Singular Value Decomposition SVD[3]	Threshold	Detects forged Region, JPEG compression	Computational cost very high

3	Principal Component Analysis PCA[4]	Precision, Recall rate, false detection	Low complexity, less number of false positives	Cannot detect spliced region
4	Local Binary Pattern LBP[5]	Neighborhood clustering	Low complexity, locates duplicate image	Cannot detect rotated and scaled images
5	Multiresolution Local Binary Patterns MLBP[6]	k-d tree method	Eliminate false matches	High time consuming for forgery detection
6	Fourier-Mellin Transform FMT[7]	Eigen Vectors	Robust to JPEG compression blurring, noise, scaling	Unable to detect when rotated via some angles
7	Discrete Fourier Transform DFT[8]	Circular window expansion and phase correlation.	Detects forged region, anti-noise capabilities	Cannot detects false matches
8	Weber local descriptor WLD[9]	Support vector machine	Robust to noise	Difficult for large size images.
9	Scale Invariant Feature Transform SIFT[10]	Threshold	Detects copy regions with geometrical transformation	False positive still higher
10	Histogram of Oriented Gabor Magnitude HGOM[12]	Correct detection ratio(CDR) and false detection ratio(FDR).	Robust against attacks like JPEG compression brightness adjustment, blurring and image rotation with low computational complexity	Cannot use large block size

IV. CONCLUSION

The copy move forgeries have taken regular place in our daily life there is an rising need of image forgery detection methods to deal with many aspects of image forensics. In this paper, have discussed image forgery detection techniques and different types of image forgeries. The basic flow of how forged region is detected is shown. The overview of different techniques that helps to detect forgeries is provided. Detection techniques have some kind of shortcomings. Some of the major problems needing attention are to reduce the computational time, increase the accuracy, and decrease the inaccuracy and the robustness against various geometric transformations. Therefore, any future research may look into these issues and algorithms are required to be developed that provide reliable solution with robust detection.

REFERENCES

[1] Fridrich, J. Soukal, D. Luk, J. (2003), "Detection of copy-move forgery in digital images", Proc. Digital Forensic Research Workshop, Cleveland, OH, USA.

[2] Cao, Y. Gao, T. Fan, L. Yang, Q. (2012), "A Robust Detection Algorithm For Copy-Move Forgery in Digital Images", Forensic Science International, vol. 214, No. 1–3, pp. 33–43.

[3] Zhao, J. and Guo, J. (2013), "Passive Forensics For Copy-Move Image Forgery Using A Method Based On DCT And SVD", Forensic Science International, Vol. 233, pp. 158–166.

[4] Popescu, A. and Farid, H. (2004), "Exposing Digital Forgeries by Detecting Duplicated Image Regions", Tech. Rep. TR2004-515, Dartmouth College, Computer Science, Hanover, Conn, USA.

[5] 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

[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, T. Memon, N. (2009), "An Efficient and Robust Method forDetecting Copy-Move Forgery", in Proceeding of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09), pp. 1053–1056, Taipei, Taiwan.

[8] Shao, H. Yu, T. Xu, M. Cui, W. (2012), "Image region duplication detection based on circular window expansion

and phase correlation", Forensic Science International, vol. 222, no. 1–3, pp. 71–82.

[9] 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.

[10] Jing, L. and Shao C. (2012), "Image Copy-Move Forgery Detecting Based on Local Invariant Feature", Journal of Multimedia, vol 7, No 1, pp. 90-97.

[11] Amerini, I. Ballan, L. Caldelli, R. Bimbo, A. Serra, G. (2013), "A SIFT-based forensic method for copy-move attack detection and transformation recovery", IEEE Transactions on Information Forensics and Security, vol. 6, issue 3, pp. 1099-1110.

[12] H. Chen-Ming, J. Lee, and W. Chen, "An Efficient Detection Algorithm for Copy-Move Forgery," Information Security (AsiaJCIS), 10th Asia Joint Conference on. IEEE, (2015).

[13] A. Edoardo, A. Bruno, and G. Mazzola, "Copy-move forgery detection by matching triangles of keypoints," IEEE Transactions on Information Forensics and Security, (2015).