A Survey of Copy-Move Forgery Detection Techniques for Digital Images

Rani Susan Oommen
Sree Buddha College of Engineering for Women, Pathanamthitta, Kerala

Jayamohan M.
College of Applied Science Adoor, Kerala, India

Sruthy S.
Sree Buddha College of Engineering for Women, Pathanamthitta, Kerala

Abstract- With the development of image editing tools, manipulations of images has become a very easy task. Copy-move forgery is one such image manipulation, where some regions in the image is copied and pasted to another region in the same image. The objective of copy-move forgery may be to conceal some unwanted features, or to add some local features which are otherwise absent. Extensive research has been done to device methods to detect copy-move forgery in both intensity domain and frequency domain. Various image analysis techniques using image moments, dimensionality reduction, texture analysis etc. has been experimented. This paper presents a study of various image forgery techniques and a survey of various attempts in copy-move forgery detection. A comparative analysis of major techniques is also presented.

Keywords – Image Forensics, copy-move forgery, dimensionality reduction dimension, hybrid detection

I. INTRODUCTION

The present era of digital revolution made it very easy to access, process and share information. However, such technological advances impose security challenges. Digital image play a significant role in different fields and technologies. Images play an important role in forensic studies and law enforcement, where images are used as authenticated proofs. Therefore verifying the integrity of images is of great importance. With the rapid advancement in the image processing software such Photoshop, Corel Draw etc., digital images can be easily manipulated and modified even by ordinary people [1]. Such intentional manipulation to cause damage or make unauthorized alterations on digital images is termed as digital Image tampering.

Image forgery can be traced back to as early as 1840s, "Self Portrait of a Drowned Man", created by Hippolyte Bayradis which is said to be the very first fake image, in which he was shown committing suicide, shown in Fig. 1a. Another example of image forgery appeared in which Abraham Lincoln's head was superimposed onto the portrait of southern political leader, John Calhoun, shown in Fig. 1b. Many other instances of image forgery could be found in the history.

Fig. 1a: Self Portrait of a Drowned Man

Fig. 1b: President Abraham Lincoln (left) and politician John Calhoun (right).

This paper is organized as follows: The different type of digital image forgery is given in Section 2. The paper provides an overview on various copy move forgery detection methods. Section 3 describes the copy-move forgery detection. The typical steps or work flow in copy-move forgery detection is given in Section 4. Some of the major

ISSN: 2319 – 1058

works done in copy move forgery detection are explained in Section 5. The conclusion and future works are presented in Section 6.

II. IMAGE FORGERY

Digital image forgery detection technique can be classified into active and passive (blind) approach [2]. The active approaches requires prior information about the original image. The image in hand is believed to be forged and the methods try to detect the forged portions within. Most of the active approach requires some pre-processing such as watermarks embedding or signature generation during image acquisition, which would limit their application [3, 4]. So, there is a need for blind forgery detection method, where no prior information about source image is required. The blind image forgery detection methods can be grouped into different categories [5]: pixel-based, format based, camera based, physical environment based, geometry based.

- Pixel Based Image forgery detection detects anomalies at the pixel level of the digital image. These techniques are categorized as; cloning, resampling, statistical and slicing.
- Format Based Image forgery detection is based on image formats, especially in the JPEG format. It is categorized into JPEG Quantization, Double JPEG, and JPEG blocking. It can detect forgery even in compressed image.
- Camera based techniques Image forgery detection includes chromatic aberration, color filter array, camera response and sensor noise to detect traces of tampering introduced at various stages of imaging process.
- Physical environment based Image forgery detection works on the basis of lightning environment under which the object or image is captured. These techniques are divided into three: Light Direction 2D, Light Direction 3D, and Light environment.
- Geometry Based Image forgery detection is divided into two, Principal points and Metric measurements, which makes measurement of objects in the world and their position relative to the camera, to detect forgery.

The digital image forgery is classified into five categories [5, 6]: Copy-move (cloning) forgery, Image Splicing, Image Retouching, Morphing, and Enhanced.

- Copy-move forgery - It 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. 2a shows copy-move attack where left side shows original image which contains three rockets and right side shows forged imaged with four rockets.

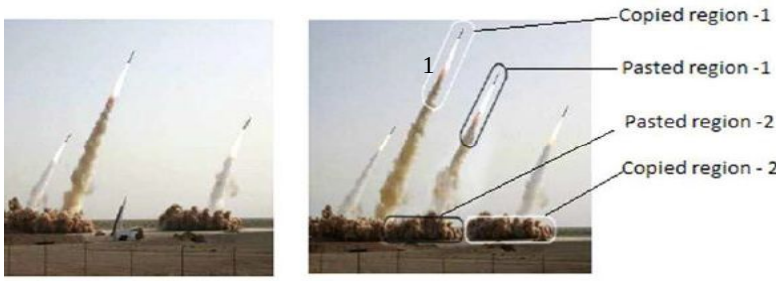

Fig. 2a: Copy-move Forgery

- Image Retouching – Different elements from multiple images are superimposed into a single composite image. Fig. 2b shows image splicing where different elements from multiple images (right) are juxtapose in a single image (left) to create forgery.

ISSN: 2319 – 1058

Fig. 2b: Image Splicing

- Image retouching – Includes slight change in the image for various aesthetic and commercial purposes. Retouching is used to enhance or reduce certain features in the image. Fig. 2c shows an example of image retouching, where real face is on the right and left shows the retouched version of it.

Fig. 2 c: Image Retouching

- Morphing- It is an image forgery where one object on image is turned into another object in the other image. Morphing is shown in Fig.2d, where left and right images are the original image and middle one is the morphed image.

Fig. 2d Morphing

- Enhanced- The original image shown is upper left corner of Fig. 2 e, followed by various enhancements such as color change, blurring of background and finally the enhanced image on the lower right corner.

ISSN: 2319 – 1058

Fig. 2e: Enhanced

III. COPY-MOVE FORGERY DETECTION

Copy-move technique is the most popular image forgery. It is tampering technique in which some region is copied and pasted to another part of the same image in order to conceal certain features or objects. Due to the nature of region-duplication, there are at least two similar regions in a tampered region.

Copy-Move forgery is performed with the intention of either making an object "hidden" from the image by covering it with a small block of background, copied from another part of the same image [7] or creates additional copy of an object already existing in the image by copying it to the desired location. Since the copied segments are part of the same image, the color palette, noise components, dynamic range and the other properties will be consistent with the rest of the image, and thus making it is very difficult for a naked human eye to detect the forgery.

Copy-move forgery detection can be either block-based or key-point based methods. In block-based methods [8], the image is divided into overlapping/non-overlapping blocks and feature vector is computed for each blocks. Similar feature vectors are identified and matched to find forged regions. In key-point based methods, image is scanned for keypoints and feature vector is calculated for every keypoints. The image is not sub-divided into blocks, the feature vectors are matched to find duplicated regions.

IV. GENERAL STEPS IN COPY-MOVE FORGERY DETECTION

In copy-move forgery, there exists a strong correlation between the copied and pasted parts which can be used as evidence for detecting copy-move forgery. The typical workflow of copy-move forgery detection is depicted in Fig. 3. Given a tampered image of size M*N, the major steps [9] involved in the detection is as follows:

A. Pre-processing

The aim of pre-processing is the improvement of image data that suppresses unwanted distortions or enhances some image features important for further detection. The given image is converted into grey-scale (color conversion) when applicable (except for algorithms that require color channels). Other pre-processing techniques includes, dimension reduction, image resizing, low-pass filtering etc. In both block-based and key-point based methods necessary pre-processing can be applied.

B. Feature Extraction

For block-based methods, feature vectors are extracted for each block. While for key-point based methods, feature vectors are computed only key-points in the image such as regions with entropy etc.

C. Matching

After feature extraction, the potential copy-move pairs are identified by searching blocks with similar features. High similarity between feature descriptors can be interpreted as duplicated regions. In block-based method lexicographically sort similar features and Best-Bin-First search method to get approximate nearest neighbour in key-point based methods helps in the feature matching.

D. Filtering

A single similarity criterion is not enough to claim the presence/absence of duplicated regions. Filtering schemes are thus used to reduce probability of false matches. Finally post-processing can be done to preserve matches that exhibit a common behaviour.

ISSN: 2319 – 1058

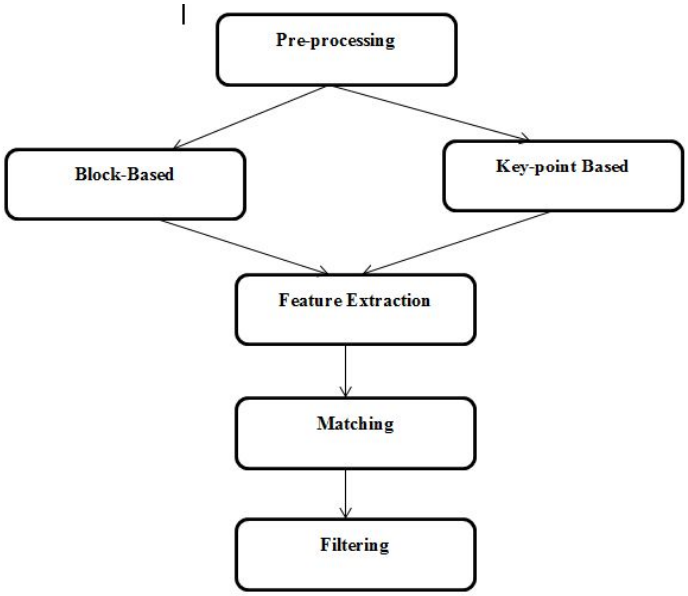

Fig. 3: Steps in Copy-Move forgery Detection

V. STUDIES ON COPY-MOVE FORGERY DETECTION

During the past few years, many works have been reported in the copy-move forgery detection. It can be generally categorized as block-based approaches, key-point based approaches, and hybrid approaches.

A. Block-Based Approaches

The block-based methods are classified as- Intensity based methods, Frequency Based methods, Dimensionality-Reduction Based methods, Moment Based, Texture Based methods.

B. Intensity Based Methods

W.Luo, J Huang, G. Qiu [10] suggested a robust copy move forgery detection method which has lower computational complexity and robust to post after-copying manipulations such as noise contamination, blurring, mixture of these operations etc. The algorithm first extracts the block characteristics features including the directional information of blocks. The feature vector list is lexicographically sorted. The search for similar blocks is done by applying a similarity measure. The correct matching block pair is found using shift vectors. Identify shift vector with highest frequency of occurrence as main shift vector (d), and regard a similar block pair as incorrect matching pair when its shift vector is much different from d. It also applies some rules to determine whether the computed matched regions are actually the forged segments.

Another method to detect region duplication was proposed by Bravo-Solorio and K. Nandi [11] , even when the cloned segment has undergone reflection, rotation or scaling. The algorithm comprised of three stages, where first stage is feature extraction in which colour-dependent feature including entropy of luminance channel of each pixel block is considered as feature vector. Second stage is search for matches, where the above feature vectors of each block is lexicographically sorted and to search for a possible match of the block, the Correlation Coefficient is computed. To reduce false matches final stage is applied, refinement which examines matches separated by similar offsets.

Lin, Chun-Wei Wang, Yang-Ta Kao [12] recommended a copy-move detection scheme which is robust to lossy JPEG compression, a Gaussian noise and rotation. To detect such forgeries, a given image is divided into overlapping blocks, a 9-dimensional feature vector is extracted is for each block and sorted using radix sort. The difference (shift vector) of the positions of every pair of adjacent feature vectors in the sorting list is computed and the accumulated number of each of the shift vectors is evaluated. Finally, the medium filtering and connected component analysis are performed on the tentative detected result to remove noise and obtain the final result.

ISSN: 2319 – 1058

C. Frequency Based Methods

J. Fridich, David Soukal and Jan Lukas suggested [13] an exhaustive search method to detect copy move forgery based on DCT coefficients. The given image is divided into blocks and DCT coefficients are extracted and stored in an array. The array is lexicographically sorted and quantized values of DCT coefficients for each block are compared. It also looks at the mutual positions of each matching block pair and outputs a specific block pair only if there are many other matching pairs in the same mutual position. The above method detect copy move region, but it will not work in noisy image.

DCT based detection method robust to multiple copy move forgery, noise contamination, Gaussian blurring, rotation up to 5 degrees, scaling and shifting was proposed by N. D. Wandji, S. Xingming, M. F. Kue [14]. In the proposed method, RGB image is first converted into YUV color space and dividethe R, G, B and Y-component into fixed sized blocks. Lexicographically sort the feature vector matrix and search for similar block pairs and output the duplicated regions.

D. Dimensionality-Reduction Based Methods

Popescu and H. Farid [16] a dimensionality reduction based copy-move forgery detection by applying PCA to blocks in the image, which is robust to additive noise or lossy compression. These blocks are lexicographically sorted and duplicated regions are detected by noting the offsets with highest occurrence. The algorithm detects copy-move regions with less false positive.

Kang and Wei introduced [17] a tamper detection approach based on singular value decomposition (SVD). SVD served to produce algebraic and geometric invariant and feature vectors. The algorithm divides the image into overlapping blocks. Then to each block apply SVD and obtain reduced-rank dimension and extract singular value feature vectors and store it in a matrix. Lexicographically sort and consecutive rows indicate identical blocks. If similarity between blocks is higher than a fixed value, copy-move tamper is detected. The method localizes the copy move tampering, has lower computational complexity and higher noise immunity.

E. Moment Based Methods

B. Mahdian and S. Saic [24] conducted a study of copy-move forgery detection based on blur moments. This method detects copy-move forgery, even when blur degradation, noise or arbitrary contrast changes are present in the duplicated regions. The algorithm proceeds as follows: First image is tiled with overlapping blocks. Then compute 24 blur invariant features from each block. Apply principal component transformation to reduce the dimension of the feature vector. Use k-d tree representation and perform block similarity analyses. Set a threshold, and blocks with similarity measure larger or equal to threshold are considered similar. In verification step, similar blocks with different neighbours are eliminated. Then create a duplicated region map that shows image regions which are likely duplicated.

S. J. Ryu, M. J. Lee, H.K. Lee [25] proposed an algorithm where features are based on Zernike moments to detect copy-move forgery in tampered images. The method first divides the suspicious image into blocks. Then a Zernike moment from each block is calculated. The magnitude of Zernike moments is invariant to rotation, also resilient to additive white Gaussian noise, JPEG compression and blurring. The computed feature is lexicographically sorted and estimate the Euclidean distance between pairs. Those blocks with distance smaller than threshold are candidates for forgery. However the method fails in detecting scaled coy-move blocks.

F. Texture Based Methods

A block based approach which exploits texture as features to detect copy move forgery was proposed by E. Ardizzone, A. Bruno, and G. Mazzola [22]. The algorithm first converts the given image into grey scale. Divides the image into blocks and extract features from each block. The authors tested five texture descriptors, namely, statistical descriptors (mean, standard deviation, skewness and kurtosis), edge histogram, Tamura descriptors (contrast, coarseness and directionality properties from Tamura set of features), Gabor Descriptors and Haralick descriptors. Blocks are sorted and similarity criterion is applied to find candidate blocks. Compute distance between spatial coordinates of candidate blocks to find matching pairs.

Quan, H. Zhang [23] proposed copy move detection method in image blocks with similar texture instead of in the whole image, which decreases the complexity of the algorithm. The algorithm first exerts pre-processing, applying image segmentation using local dimension estimation and then matches source and target regions in the image with the same texture. In forged digital image, forgery must occur in area with the same texture. Then it computes difference vector and uses estimated local dimension to locate the copy-move forged region.

G. Key-point Based Approaches

ISSN: 2319 – 1058

X. Pan and S. Lyo [18] proposed a detection method based on matching image SIFT (Scale-Invariant Feature Transform) features. This method is robust to transforms such as rotation, scaling and less susceptible to noise and JPEG compression. The algorithm includes four steps. First, identify the key-points and collect the SIFT feature vector for each key-points. Then SIFT key-points are matched and prune matches to reduce the false matches. Estimate region transforms and based on the correlation coefficient identify the duplicated regions.
SURF (Speeded-Up Robust Feature Extraction) based method of Copy-move Forgery in flat regions was suggested by G. Zhang, H. Wang [26]. The algorithm detects copy-move forgery by extracting SURF key-points from the image. Then feature matching and pruning is done. Finally estimate region transforms and identify duplicated regions using correlations adjusted using estimated transforms. The method can detect region duplication in non-flat region and is rotation invariant.

H. Hybrid Approaches

F. Liu and H. Feng [19] proposed a DWT-SVD hybrid approach for copy-move forgery detection. It can detect multiple copy-move forgery and precisely locate duplicate regions, even when image is distorted by Gaussian blurring, JPEG compression and their mixed operations. The algorithm first convert the given into grey-scale and apply 1-level DWT to get LL sub-band. It then divides LL sub-band into overlapping blocks. Perform SVD on each block to get the dominant feature. Sort blocks based on dominant feature into bucket groups. Processing done on each bucket gives the matching duplicated blocks.

DCT-SIFT based copy-move forgery detection was introduced by R. Singh, A. Oberoi [20]. The algorithm uses a hybrid approach based on block based and feature based technique to increase the accuracy rate of forgery detection. The given image is converted to grey-scale. It employs DCT and SIFT to extract features from the image and matching those collected features to detect forgery and to localize forged regions in the digital image. This method can detect multiple forgeries with minimum false matches.

Another hybrid approach based on DWT and PCA-EVD to detect copy-move forgery detection was proposed by M. Zimba, S. Xingman [21]. The algorithm first applied DWT and extracted low frequency sub-band, while reducing the dimension of the image. Divide the image into blocks and perform PCA-EVD on each row vector to get reduced dimension feature vector, which is lexicographically sorted to find similar blocks. This method is not invariant to post-processing manipulations such rotation, rescaling and high compression.

A SIFT and Zernike moments based region duplication detection was suggested by Z. Mohamadian, A. Pouyan [27]. The algorithm first applies SIFT method to extract special points in the image which are invariant to rotation and scaling. It first extracts SIFT feature and a matching operation is performed. False alarms of forgery is dealt using hierarchical clustering and based on a definite threshold value.The image is considered forged only when three similar feature points matched.

VI. CONCLUSION& REMARKS

Copy-move forgery detection is one of the main challenging tasks in digital image forensics. Over the recent years, several works have been carried out to effectively detect the copy-moved regions. We discussed different digital image forgery, focusing mainly on copy-move forgery and have a brief survey on various copy-move detection algorithms. We discussed some previous works in block-based, key-point based and hybrid approaches to detect copy-move forgery detection.

It is seen that block-based methods are more efficient than key-point based methods. There are several hybrid approaches that show improved performance in the detection.

REFERENCES

[1] Stephen Edwin Coleman, “Digital Photo Manipulation: A Descriptive Analysis of codes of Ethics and Ethical Decisions of Photo Editors,” 2007.

[2] B.L.Shivakumar, Lt. Dr. S.Santhosh Baboo, “Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods,” Global Journal of Computer Science and Technology, 2010, Vol. 10, Issue 7, pp. 61-65.

[3] D. Kundur, D. Hatzinakos, “Digital watermarking for tell-tale tamper proofing and authentication,” Proc. IEEE, vol 8, no. 7, 1999, pp. 1167-1180.

[4] J. Fridich, “Methods For Tamper Detection In digital Image,” Proc ACM Workshop on Multimedia and Security, Orlando,, FL, October 30-31, 1999, pp. 19-23.

[5] M. D. Ansari, S. P. Ghrera, V. Tyagi, “Pixel-Based Image Forgery Detection: A Review,”IETE Journal of Education, 55:1, 40-46.

ISSN: 2319 – 1058

[6] S. A.Thajeel, G. Sulong, "A survey of copy-move forgery detection Techniques," Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645.
[7] S. Sharmila, S. Prajakta, S. Hiral, "Image Forgery Detection Techniques for Forensic Sciences,"ijournals, ISSN-No: 2347-4890,vol 2, issue 8, August 2014.
[8] Resmi S, Chithra A S, "Recent Block-based Methods of Copy-Move Forgery Detection in Digital Images," International Journal of Computer Applications (0975 – 8887) Volume 89 – No 8, March 2014.
[9] V. Christlein,, C. Riess, J. Jordan, C. Riess, E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," IEEE Transactions On Information Forensics And Security, Vol. 7, No. 6, December 2012.
[10] W Luo, J Huang, and G Qiu, "Robust detection of region-duplication forgery in digital image," Proc.of ICPR, Aug. 2006
[11] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affectedby reflection, rotation and scaling," in *Proc. Int. Conf. Acoustics,Speech and Signal Processing*, May 2011, pp. 1880–1883.
[12] H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection,"*WSEAS Trans. Signal Process*., vol. 5, no. 5, pp. 188–197, 2009.
[13] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy-move forgeryin digital images," in *Proc. Digital Forensic Research Workshop*,Cleveland, OH, Aug. 2003.
[14] N. D. Wandji, S. Xingming, And M. F.Kue, "Detection Of Copy-MoveForgery In Digital Images Based OnDct," International Journal OfComputer Science Issues (Ijcsi), Vol.10, 2013.
[15] L. Li, S. Li,H. Zhu, S. Chu, J. F. Roddick, and J. Pan, "An efficient scheme for detecting copy-move forged images by local binarypatterns," *Journal of Information Hiding and Multimedia SignalProcessing*, vol. 4, no. 1, pp. 46–56.
[16] A. C. Popescu, H. Farid. "Exposing digital forgeries by detectingduplicated image regions," Technical Report TR 2004-515, DartmoughCollege, Aug. 2004
[17] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in *Proc. Int. Conf. Computer Science and Software Engineering*, 2008, vol. 3, pp. 926–930.
[18] Pan, X., Lyu, S.: 'Detecting image region duplication using SIFT features'. 2010, IEEE Int. Conf. on Acoustics Speech and Signal Processing (ICASSP), 2010, pp. 1706–1709.
[19] Feng Liu1, Hao Feng, "An efficient algorithm for image copy-move forgery detection based on DWT and SVD," International Journal of Security and Its Applications Vol.8, No.5 (2014), pp.377-390.
[20] R. Singh, A. Oberoi, N. Goel, "Copy Move Forgery Detection on Digital Images," *International Journal of Computer Applications (0975 – 8887) Volume 98– No.9, July 2014.*
[21] M. Zimba, S. Xingming, "DWT-PCA (EVD) Based Copy-move Image Forgery Detection," International Journal of Digital Content Technology and its Applications. Volume 5, Number 1, January 2011.
[22] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy-move forgerydetection via texture description," in *Proceedings of the 2nd ACMworkshop onMultimedia in Forensics, Security and Intelligence(MiFor '10)*, pp. 59–64, ACM, October 2010.
[23] X. Quan, H. Zhang, "Copy-move forgery detection in digital images based onlocal dimension estimation," IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (Cyber Sec), June 2012.
[24] B. Mahdian and S. Saic, "Detection of copy-move forgery using amethod based on blur moment invariants," Forensic science international,vol. 171, no. 2, pp. 180-189, Sep. 2007.
[25] S.-J. Ryu, M.-J. Lee, and H.K. Lee, "Detection of copy-rotate-moveforgery using Zernike moments," in Information Hiding. Berlin,Heidelberg: Springer, 2010, pp. 51-65.
[26] G. Zhang, H.Wang, "SURF based Detection of Copy-Move Forgery in Flat Region," International Journal of Advancements in Computing Technology (IJACT) Volume4, Number17, September. 2012 doi:10.4156/ijact.vol4.issue17.61S
[27] Z. Mohamadian, A. Pouyan, "Detection of Duplicated Forgery in Digital Images In Uniform and Non Uniform Regions," UKSim 15th International Conference on Computer Modelling and Simulation, 2013.
[28] S. A.Thajeel, G. Sulong," State Of the Art Of Copy-Move ForgeryDetection Techniques: A Review," IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013.