INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 1)
Available online at: www.ijariit.com

Review on copy move forgery image detection and classification

Sharika Ahad
manshguide@gmail.com
Yamuna Institute of Engineering and Technology, Yamunanagar, Haryana

Sunil K. Panjeta
Panjetasunil@gmail.com
Yamuna Institute of Engineering and Technology, Yamunanagar, Haryana

ABSTRACT

Digital image is an essential part of today's everybody life. We use digital images in various fields like social networking sites, e-commerce companies, jobs, courtrooms, academics, insurance fields etc. Any unauthorized person can easily make changes in anybody digital image and use it in place of authorized person and takes benefits. To identify the original and tampered digital images we need some detection techniques to recognize the image is actual or tampered.

Keywords— *Copy, Optimization, Blocks Features*

1. INTRODUCTION

Image tampering is the way through which anyone can create duplicate or altered image. The aim of doing tampering is to get benefits by offering tampered things. There are many commercial and open source image editing software's are available that are used to manipulate the digital images. By using these software's anyone can easily change the content without effecting their quality.

Authenticity of digital images is a major issue in image forensics field. In the recent years, a large number of approaches related to image tampering is occurred such as copy-move, image splicing, image retouching etc. copy-move is one of the generally used image tampering method. In copy-move part of the image is copied and pasted on another part of the same image. Tampered images look very similar to original images, it's very complicated to judge the actual or tampered image. The copied area has the following properties such as color palette, noise components, dynamic range etc. By using various types of techniques to create tampering in digital images, unauthorized person tries to create the copied area like an actual appearance of the same image.

1.1 Need of Digital Image Tampering Detection

These are some fields where tampered image are produced in large amount: In Medical field there are many types of cases where any person produced tampered medical image as verification for unhealthiest person and claim of disease. In courtrooms, there are various cases in which, tampered images are produced as an evidence and criminal person not punished due to lack of evidence. There are many fraud companies that create their sites similar to the actual one, people joined with hope but they cheat them.

1.2 Digital Image Tampering Types

Digital image tampering is not an easy task before a decade but today's availability of various open source image editing software tools makes it an easy task. It's very tough to maintain the authenticity of digital images. Following are some common method of digital image tampering:

1.2.1 Copy-Move Image Forgery: Copy-move is one of the mostly used image tampering method. In copy-move, some part of a digital image is copied and pasted to another part of the same digital image. By doing this process the unauthorized person tries to maintain the appearance of tampered image to similar to the actual image.

Fig. 1: (a) Original Image (b) Copy-Move Forgery [5]

1.2.2 Image Splicing: Image splicing is another popular image tampering method. In this method two digital images are combined to a single image. One part of an image is pasted to more than one part of another image to create a single one. It's very difficult to judge the image is tampered or not.

Fig. 2: (a) Original Image1 (b) Original Image2 (c) Spliced Image [5]

1.2.3 Image Resampling: Image Resampling is also another type of image tampering method by which some changes are made in the image like color, weather and blurred background. Some geometric transformations are also made in image retouching such as rotation, scaling, stretching etc.

Fig. 3: (a) Original Image, (b) Image Resampling [5]

1.3 Mechanisms Used for Image Tampering Detection
Image Tampering detection techniques mainly divided into two major parts:

1.3.1 Active Approach: Active approach needs surplus information embedded in the digital image. To identify the digital image is tampered or not check digital watermark and digital signature that is embedded in digital images. Digital watermark and digital signature confirm the originality of digital images. Additional information (i.e. digital watermark and digital signature) is inserted into digital image at the time of capturing or later by authorized personnel.

1.3.2 Passive Approach: In Passive approach no need of additional information to recognize the tampering in digital images. The passive approach finds out the pastiche by extracting the internal features within the digital images depends on the identification of source device and detection of tempering. This approach is categorized into two parts: Dependent and Independent Tampering

Dependent Image Tampering: Dependent images tampering performs two types of image manipulations that is: image copy-move and image splicing

(a) Copy-Move Image Tampering: In copy-move image tampering one part of the image is copied and pasted on another part of the same image. This is one of most popular image forgeries in digital image tampering. Many unauthorized users take advantage of copy-move forgery.

(b) Image Splicing Tampering: In image splicing one or more part of an image is combined with another image. This one is also popular tampering method in digital images. Two digital images are combined to each other and represent a new digital image and take benefits. [5]

2. RELATED WORK

He Yan et al. [1] Proposed an image classification approach by using CNN and fusing. It has vast range of use like content-based image classification, object and scene recognition. The most challenging problems occurs in image classification is due to the diverse characteristics in images like scale and universal perspective the object's internal deformation, complicated background, illumination etc. A novel approach is introduced to combine the deep latent features in CNN model to improve the image classification. Latent features are extracted from a pre-trained model. Combined classifier performs better than individual classifiers.

Yuan Rao et al. [2] presented a new tampering detection method based on deep learning technique that automatically learn hierarchical representations form the RGB color images. Use 30 basic high pass filters in SRM which helps to improve the effect of complex image contents and increases the convergence of network. CNN work as local patch descriptor. Extract dense features by using pre-trained CNN. Feature fusion method is use to obtain the discriminative features for SVM classification.

Sundus Farooq et al. [3] Proposed a generic approach for image forgery detection and found that image forgery is popular area form research perspective. Use spatial rich model (SRM) in combination textural feature i.e. local binary pattern (LBP). Multiclass classifier is used to classify the features into different forgeries classes. Using LBP in conjunction with co-occurrence matrices make the model capable enough to detect almost all types of forgeries with improved detection accuracy.

Peizhang Liu et al. [4] describes an approach for texture image retrieval and classification and found that in textural image retrieval and classification LBP operator and its variants work as an image feature extractor. Extract textural information of an image by using neighboring pixel values. CIF and LBP based features performs better in image retrieval and classification, the CIF indemnify the problem of the LBP based operator on describing the color information.

Haoyu Zhou et al. [5] formulated the image forgery detection method using histograms and found that copy-move is one of the most widely used tampering method. The proposed method is based on the color moments and five descriptors (i.e. color moments, color layout descriptors, color and edge directivity descriptor etc.) use to improve the detection accuracy. The method divides images into fixed size overlapping blocks. Clustering operation divides total search space into smaller pieces with similar color. The presented technique ensures the robustness against some post-processing operations.

Mohammad et al. [6] founded that digital images are easily tampered by using various photo editing software's so authenticity and integrity of digital images are the main concern. Present new method, combination of Dyadic Wavelet Transforms (DyWT) with Scale Invariant Feature Transform(SIFT), by using DyWT with SIFT, easily extract more key points and capable to efficiently detect the copy-move forgery. Present technique is high matching rate and robust against attack and pre-processing techniques.

Shahana et al. [7] presented that security of digital images in an essential part of image security because high resolution camera, photo editing software easily manipulate images. The main focus on one of the common image manipulations such as image splicing. Detect inconsistencies among various images and identified with the help of pixel and edge-based illuminant color estimation regions. Extract shape and color features by using illuminate extractors. It mainly used pixel and edge methods. Canny edge detector and HOG is used to identified the forgery. By using this approach accuracy of forgery detection is improved.

Sondos M. Fadl et al. [8] founded that copy-move (CM) is commonly used tampering in digital images. Use Block Matching (BM) technique to detect copy move forgery. Extract essential features for each block with the help of polar coordinate system. The main focus on frequency of each block is based on Fourier Transform.by using polar representations blocks that transform geometrically have similar polar values and little shift in block columns and rows. The precision rate of

Polar Copy- Move (PCM) system perform better than previously available techniques.

Ashwini et al. [9] Proposed an approach which is based on the pixels for detection and also presents the irregularity at pixel level in forged images. To detect forgery, use image retrieval feature extraction method. To obtain feature vectors form the tampered image, use Auto Color Correlation (ACC) feature extraction technique, also useful in detecting forged region. This method easily identifies the tampered images and performs better than previously available methods.

Anil et al. [10] presented a new approach called as Scaling Robust method of Copy-Paste Tampering for digital Image Forensics and found that authenticity of digital images is a critical task. For copy-paste tampering, propose a passive scaling robust method. No need of dimensionality reduction and any sorting methods for feature vectors. Performs better compare to other block-based methods.

Nor Bakiah et al. [11] founded that how authenticity of an image maintains against various tampering software's. Copy-move one of the common types of digital image tampering software. Focus on block or key-point based feature extraction and feature matching to find out the digital image tampering.by using these methods we can easily classify the tampered or non-tampered images.

Chen-Ming et al. [12] described that a familiar image tampering method (i.e. copy move). Introduce the new method that first break tampered image into fixed size non-overlapping blocks and apply Gabor filter at each block. HOGM extract statistical feature of overlapping blocks. HOGM performs better compare to other existing methods.

Rani Susan et al. [13] Presented Fractal dimension and Singular Values approach for Image Forgery Detection and Localization and found that authenticity of digital image is a major factor and one of the mainly used forgery techniques i.e. copy-move. Present a novel approach that is a combination of Local Fractal Dimension and Singular Value Decomposition using this approach easily detect the localization and duplicate areas. Work on texture complexity is not an easy task. Fractal dimension with SVD effectively identified the tampering area. Effectively manage the computation time by using B^+ tree arrangement of image blocks. Sorted according to local fractal dimension. Presented approach is robust against copy operation and multiple tampering problems.

Vinoth S. et al. [14] proposed a Neural Network model and found that manipulation in digital images is an easy task because of there are various image editing software's are available nowadays, so authenticity of an image is a crucial task. Present the new method that use nonlinear model (back propagation neural network) to represent the linear array. Use K-LDA to reduce dimensionality of collected features. Classifier are used for training and testing of images. Performance in image classification achieves better accuracy compare to existing methods.

Reshma et al. [15] presented Key point extraction Using SURF algorithm and found that copy-move one of mostly used image tampering approach. Present new technique that easily identified the tampered area, first segment the images into various patches and identified the tampered image by using matching technique. Patch matching is done by using affine transform matrix and in second stage use Expectation Maximization Algorithm that easily classify the tampered image. This Procedure effectively identified the tampered area and improve the performance.

3. CONCLUSION

easy task because of there are various image editing software's are available nowadays, so authenticity of an image is a crucial task. Present the new method that use nonlinear model (back propagation neural network) to represent the linear array. Use K-LDA to reduce dimensionality of collected features. Classifier are used for training and testing of images. Performance in image classification achieves better accuracy compare to existing methods.

Table 1: Existing Scheduling Model

Paper name	Algorithm	Parameters/Accuracy	GAP
Asghar, K., Habib, Z., & Hussain, M. (2017). Copy-move and splicing image forgery detection and localization techniques: a review. *Australian Journal of Forensic Sciences*, *49*(3), 281-307.	CNN is a kind of neural network that shares weights among neurons in the same layer. CNN is good at discovering spatially local correlation by enforcing a local connectivity pattern between neurons of adjacent layers	90%	Not find the key features only find the texture features
Yang, F., Li, J., Lu, W., & Weng, J. (2018). Copy-move forgery detection based on hybrid features. *Engineering Applications of Artificial Intelligence*, *59*, 73-83.	combine KAZE, a robust interest point detector, with SIFT to obtain more feature points	90.27%	Not improve the matching procees
Lin, C., Lu, W., Huang, X., Liu, K., Sun, W., Lin, H., & Tan, Z. (2019). Copy-move forgery detection using combined features and transitive matching. *Multimedia Tools and Applications*, *78*(21), 30081-30096.	combined features which are composed of LIOP and SIFT are proposed	93%	• It improves the feature but not optimize or refine the features • Ignoring the efficient matching

4. REFERENCES

[1] He Yan, Xueliang Liu, Richang Hong, "Image Classification via fusing latent deep CNN feature",978-1-4503-4850,2016.

[2] Yuan Rao, Jiangqun Ni, "A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images", IEEE International WIFS 978-1-5090-1138-4/16(2016).

[3] Sundus Farooq, Muhammad Haroon Yousaf, Fawad Hussain, "A generic passive image forgery detection scheme using local binary pattern with rich models", Computers and Electrical Engineering 1-14,2017.

[4] Peizhong Liu, Jing-Ming Guo et.al, "Fusion of Colour Histogram and LBP based Features for Texture Image Retrieval and classification", Information Sciences 2017.

[5] Devanshi Chauhan, Dipali Kasat, Sanjeev Jain, "Survey on Key point-based Copy-move Forgery Detection Methods on Image, Procedia Computer Science 85,206-212,2016.

[6] Mohammad Farooq Hashmi, Vijay Anand, Avinas G. Keskar, "Copy Move Image Forgery Detection Using an Efficient and Robust method combining Un-decimated wavelet Transform and Scale Invariant Feature Transform", Aasri Procedia 9,84-91,2014.

[7] Shahana N Youseph, Rajesh Roy Cherian, "Pixel and Edge based Illuminant Color Estimation for Image Forgery Detection", Procedia computer Science 2015.

[8] Sondos M Fadl, Noura A Semary, "Robust Copy Move forgery revealing in digital images using polar polar coordinate system", Neurocomputing 2017.

[9] Ashwini M Malviya, Siddharth A Ladhake, "Pixel based Image Forensic Technique for Copy-move forgery detection using auto color Correlogram", Procedia Computer Science 2016.

[10] Anil Dada Warbhe, R.V. Dharaskar, V.M. Thakare, "A Scaling Robust Copy-Paste Tampering Detection for Digital Image forensics", Procedia Computer Science 2016.

[11] Nor Bakiah Abd Warif, Ainuddin Wahid Abdul Wahab, "Copy-move forgery detection: Survey, challenges and future directions 2016.

[12] Chen-Ming Hsu, Jen Chun Lee, "An Efficient Detection Algorithm for Copy-Move Forgery", IEEE978-1-4799-1989 (2015).

[13] Rani Susan Oommen, Jayamohan M, Sruthy S, "Using Fractal and Singular Values for Image Forgery Detection and Localization", Procedia Technology 24,1452-1459,2016.

[14] Vinoth S, E.S. Gopi, "Neural Network Modeling of color array filter for digital forgery detection using Kernel LDA", Procedia Technology 10,498-504,2013.

[15] Reshma Raj, Niya Joseph, "Keypoint Extraction Using SURF Algorithm for CMFD", Procedia Computer Science 93,375-381,2016.

[16] Beste Ustubioglu, Guzin Alutas, "A new copy move forgery detection technique with automatic threshold determination", International Journal of Electronics and Communications (2016).

[17] Haodong Li, Weiqi Luo, Xiaoqing Qiu, "Image forgery Localization via Integrating Tampering Possibility Maps", IEEE Transactions on Information Forensics and security (2016).

[18] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, "Robust Hashing for Image authentication using Zernike Moments and Local Features", IEEE transactions on Information forensics and security, Vol.8, No.1, January 2013.

