International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
© Global Society of Scientific Research and Researchers
http://ijcjournal.org/

A Study on Image Forgery Detection Techniques

Shijo Easow[a*], Dr. L. C. Manikandan[b]

[a]*M.Tech, Student,Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India*
[b]*Professor, Dept. of CSE,Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India*
[a]*Email: shijoeasow@gmail.com*
[b]*Email: lcmanikandan@gmail.com*

Abstract

In this contemporary world, digital image plays a vital role in several application areas. Image forgery means that handling of the digital image to hide some significant or helpful information of the image. The aim of this study is to provide the knowledge of image forgery and its detection techniques for the new researchers.

Keywords: Digital image; JPEG; Image forgery detection techniques; Digital signature; Digital water marking.

1. Introduction

Digital image is an image or picture represented digitally. It is a numeric representation, normally binary, of a two-dimensional image. The digital image is a crucial means that to distribute information in Internet, that is extensively used in almost every field [1]. Most of digital images involve business secrets and even national security. Internet development and multimedia easy distribution make the content security of pictures become a crucial issue for scientists and engineers. Image processing may be a technique to convert a picture into digital kind and perform some operations on that, in order to get a better image or extract some helpful data from it. Image processing is one of the researches that attract the interest of wide range of researchers. Image processing, mostly deals with processing of images, pictures, video etc. Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame the output of image processing may be either an image or, a set of characteristics or parameters related to the image [5]. Image processing deal with a range of aspects like image zooming, image segmentation, image enhancement, video and image compression and transmission (JPEG, MPEG, HDTV, etc.)[9], computer vision (robots, license plate reader, tracking), commercial software's (Photoshop) and many more.

----

* Corresponding author.

2. Image Forgery Detection Techniques

Digital image forgery detection field has grown fundamentally to battle the issue of image distortion in various areas like legitimate administrations, medical sciences; legal sciences [14]. Image Forgery Detection (IFD) techniques applied for both Copy-Move and spliced images. For the Copy-Move images, the classification depends on variations in processing input images with or without transformation before extracting the image features. For the spliced images, groups of detection techniques based on image features or camera features are summarized [2]. Forgery identification determines the genuineness of images. Image forgery detection techniques are classified into two. They are:

2.1. Active Forgery Identification Techniques

An active forgery detection method needs pre-extracted or pre-embedded data. Digital signature and Digital watermarking [18,17] are commonly known methods used in active approach [24].

2.1.1. Digital signature

Digital signature is one of the active methods used for detecting image forgery or tampering. Representing the authenticity of digital document using a kind of mathematical format is named as digital signature. In digital signature a robust bits are extracted from the original image. An image is partitioned of into blocks of 16*16 pixels. A secret key k is employed to get N random matrices with entries uniformly distributed in interval [0, 1]. A low pass filter is applied on every random matrix frequently to obtained N random smooth pattern [26]. System produce digital signature by applying signing process on digital image.

2.1.2. Digital watermarking

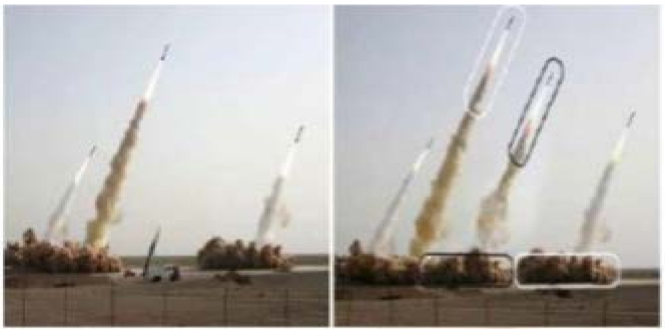
Watermarking is also used for image forgery detection. In Checksum schema that it can add data into last most significant bit of pixels. A maximal length linear shift register sequence to the pixel data and so determine the watermark by computing the spatial cross-correlation function of the sequence and also the watermarked image. These watermarks are designed to be undetectable, or to blend in with natural camera or scanner noise. Visible watermarks also exist. In addition to this, a visually undetectable watermarking schema is also available which can sense the modification in single pixels and it can find wherever the modification occur [2]. Active techniques have some disadvantages because they required some human involvement or specially equipped cameras. To overcome this drawback a passive authentication has been proposed.

2.2. Passive Forgery Detection Techniques

Passive methods, also known as blind methods, only uses the image itself for its authentication and integrity [16]. The method assumes that although there may be no visual clues of tampering in the image, but tampering may disturbs the underlying statistics property because of the Noise inconsistency, Blurring of image, Image sharpening [15], Forgery through copy-move [12] and Image inpainting [10] etc. Forgery dependent techniques are proposed to differentiate just certain kind of forgeries, like splicing those are dependent on the sort of forgery carried out on the picture [20]. Forgery independent techniques identify forgeries that are independent from fraud but in view of artifact traces left behind due to the procedure of sharpening, blurring and because of inconsistencies due to shading and light effects. The passive forgery detection techniques are:

2.2.1. Copy-move forgery detection

Copy move forgery is a method of creating a compound picture by cutting some object from image and adding it to the same image, sees in Fig 1. Copy-move forgery detection techniques are of three types.



(a) Original image (b) Copy-move image

Figure 1: Copy-move Forgery

2.2.1.1. Brute force method

Brute force method is based on exhaustive search and auto correlation technique. In exhaustive search, image is used to examine matching segment with circularly shifted versions. As it makes such large number of comparisons, its computational unpredictability is high. Autocorrelation verify location change.

2.2.1.2. Block based method

Block based approach use the algorithms such as Discrete Wavelet Transform (DWT), Principle Component Analysis (PCA), Singular Value Decomposition (SVD) and Discrete Cosine Transform (DCT) [13].

2.2.1.3. Keypoint based method

Keypoint based method uses scale and rotation invariant feature detector and descriptor algorithms which are Speeded-up Robust features (SURF) and Scale Invariant feature Transform (SIFT) .

2.2.2. Image splicing forgery detection

Copying a section of an image and pasting it onto another image is named as image splicing, see in Fig 2.

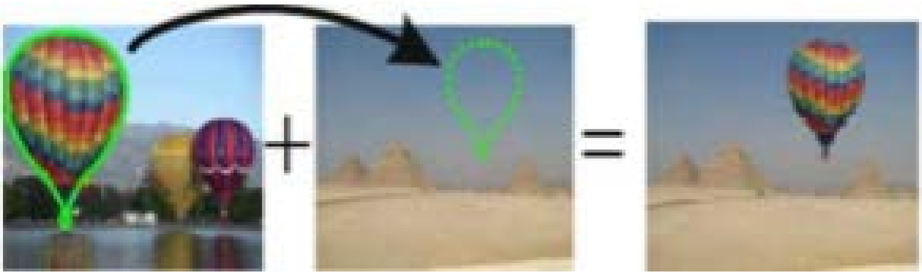


Figure 2: Image splicing

Image Splicing includes union of a minimum of two pictures to make a fake image. If the pictures with contrasting foundation are combined then it turns out to be very hard to make the borders and boundaries incoherent [6]. Image splicing is a process in which it crops and pastes regions from the same or different images. Digital photomontage uses image splicing so that two images can be sticked together using tools like Photoshop.

3. Generalized Schema for Image Forgery Identification

The principle target of blind forgery detection technique stays to classify a given picture as real or altered. The schema of image forgery identification procedure is shown in Fig.3.

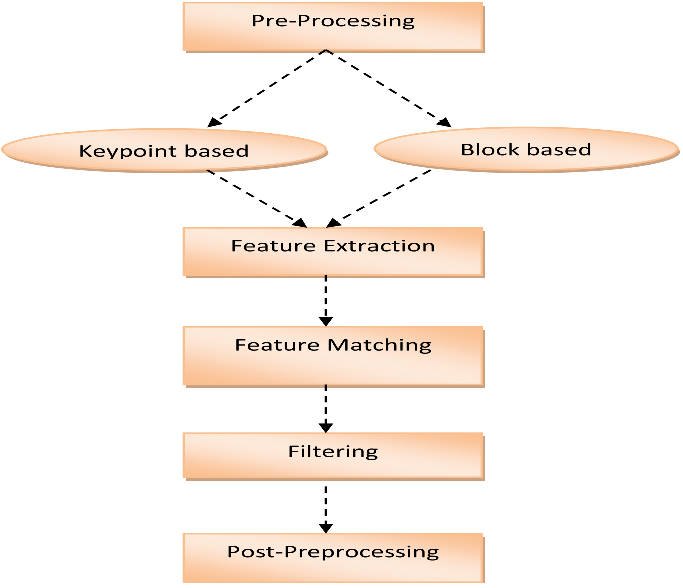


Figure 3: Generalized schema for image forgery detection

Image Preprocessing: Image preprocessing is the first phase. Some preprocessing is performed on the picture under deliberation like image filtering, image enrichment, trimming, change in DCT coefficients, RGB to grayscale transformation before handling the image to feature extraction procedures [7].

Feature Extraction: Selection of features for every class separates the image-set from different classes however in the meantime stays constant intended for a specific class chosen. The attractive element of the chosen set of features is to have a tiny measurement so that computational complexity can be diminished and have an wide distinction with other classes [8].

Selection of Classifier: Depending upon the feature-set that is extracted in feature extraction, appropriate classifier is either selected or composed. The large training sets will yield the improved performance of classifier [3,21].

Classification:-The only reason behind classification is to determine if the image is original or not. Neural systems [23], LDA [22] and SVM [25] are classifiers used for this purpose.

Postprocessing: Some forgeries will possibly require post processing that include manipulations like localization of copy locales [19,11] .

4. Block Diagram Of Image Forgery Detection

The block diagram of image forgery detection is shown in Fig.4. The input image is separated into various overlapping blocks of different shape and then the feature extraction from every block takes place. The sorting is done based on the features so that the region with same features can be easily located and remaining is considered as forged points. And last some morphological operation is applied so that it detects the forged region [4].

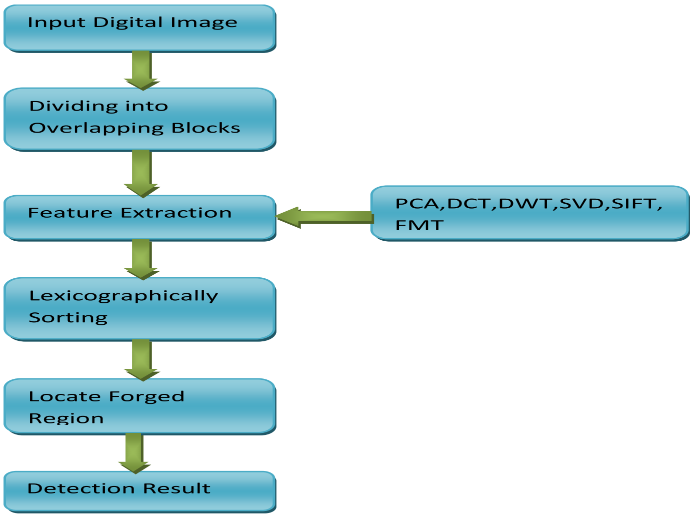

Input Digital Image
Dividing into Overlapping Blocks
Feature Extraction
PCA,DCT,DWT,SVD,SIFT, FMT
Lexicographically Sorting
Locate Forged Region
Detection Result

Figure 4: Block diagram of image forgery detection

Discrete Wavelet Transform (DWT),Discrete Cosine Transform (DCT), Principle Component Analysis(PCA),Singular Value Decomposition (SVD), Scale Invariant Feature Transformation (SIFT) and Locally Linear Embedding (LLE) are the different techniques that help to detect forgery. Copy-move forgery detection scheme using adaptive over segmentation and feature point matching. An image is divided into non overlapping blocks with the help of DWT method. The features are extracted from the blocks using SIFT method and last to detect the forged region properly a morphological operation is applied, with low computational expenses and high accuracy and recall rate. Down-sampling, scaling, rotation and JPEG compression operations are also detected. Spliced forgery can be detected with the help of this approach.

5. Conclusion

In this paper, image forgery detection, different kinds of image forgery techniques like Active and Passive are mentioned. The summary of various techniques that helps us to detect forgeries.

References

Article in a Journal

[1]. Xiaoqiang zhang and Xuesong wang, (November 2018), "Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem." IEEE Access, vol.6.

Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8528336

[2]. Shwetha B and S V Sathyanarayana, (2017), ''Digital image forgery detection techniques: a survey.**"** ACCENTS Transactions on Information Security, Vol.2 (5). Available:https://www.accentsjournals.org/paperInfo_online.php?journalPaperId=926&countPaper=251

[3]. M.Y.Munirah,N.M.Nawi,N.Wahid and M.Shukra, (2016), "A comparative analysis of feature selection techniques for classification problems." ARPN Journal of Engineering and Applied sciences, pp.13176-13187.
Available:http://www.arpnjournals.org/jeas/research_papers/rp_2016/jeas_1116_5365.pdf

[4]. Charmil Nitin Bharti and Purvi Tandel, (2016), "A Survey of Image Forgery Detection Techniques." IEEE WiSPNET. Available: https://ieeexplore.ieee.org/document/7566257

[5]. Vijay Chondagar,Harshiv Pandya and Mehul Panchal, (2015), ''A Review: Shadow Detection and Removal." International Journal of Computer Science and Information Technologies, Vol. 6(6). Available: https://pdfs.semanticscholar.org/6b2c/8d74727f62569f8b0397deb7512ddf944d75.pdf

[6]. R.W.Ibrahim, Z.Moghaddasi, H.A.Jalab and R.M.Noor, (2015) "Fractional differential texture descriptors base on the mach ado entropy for image splicing detection." International Journal of Computer Science issues, pp.4775-4786.

Available: https://pdfs.semanticscholar.org/49d5/b0b62fca0b20680697aa9238467f3f33f516.pdf

[7]. A. Makandar and B. Halalli, (2015), "A review on preprocessing techniques for digital mammography images." International Journal of computer applications, pp.0975-887. Available:https://pdfs.semanticscholar.org/82f6/787a9b2e703feb3abb3b3e728dc8702fb637.pdf

[8]. A.Phkan and M.Borah, (2014), "A survey paper on the feature extraction module of offline handwriting character recognition." International Journal of computer Engineering and Applications,

pp.51-60.

Available: https://pdfs.semanticscholar.org/c9d6/e01e189d81f3ad2f08cabbcbd12cdf92db90.pdf

[9]. L.C.Manikandan and Dr.R.K.Selvakumar, (2014), “A New Review on H.264 Video Coding Standard.” International Journal of Scientific Research,Vol.3, Issue.9.

Available:https://www.worldwidejournals.com/international-journal-of-scientific-research (IJSR)/articles.php?val=MzkxNA==&b1=189&k=48

[10]. Y.Q.Zhao, M.Liao, F.Y.Shih and Y.Q.Shi, (2013), “Tampered region detection of inpainting JPEG images.” International Journal on light electron optics, pp.2487-2492. Available:https://www.researchgate.net/publication/256821420_Tampered_region_detection_of_inpainting_JPEG_images

[11]. V.Christlein, C.Riess, J.Jordan and E.Angelopoulou, (2012) “An evaluation of popular copy-move forgery detection Approaches.” IEEE Transactions on information forensics and security, pp.1841-1854. Available: https://arxiv.org/pdf/1208.3665.pdf

[12]. F.Peng,Y.Nie and M.Long, (2011) “A complete passive blind image copy-move forensics scheme based on compound statistics features.” International journal of Fornsic science, pp.21-25.

Available: https://www.ncbi.nlm.nih.gov/pubmed/21726968

[13]. B.Soloria and A.K.Nandi, (2011), “Automated detection and localization of duplicated regions affected by reflection, rotation and scaling in image forensics.” International Journal of signal Processing, pp.1759-1770. Available: https://dl.acm.org/citation.cfm?id=1975324

[14]. B.Mahdian and S.Saic, (2010), “Blind methods for detecting image fakery.” IEEE Aerospace Electron System Management, pp.18-24.

Available: https://ieeexplore.ieee.org/document/5467652/authors#authors

[15]. Z.Y. and N.R.Cao Gang, (2009), “Detection of image sharpening based on histogram aberration and ringing artifacts.” IEEE ICME, pp.1026-1029.

Available: https://ieeexplore.ieee.org/abstract/document/5202672

[16]. H.Farid, (2006), “A survey of image forgery detection.” IEEE Signal Processing Magazine, pp.6-25. Available: http://ceng2.ktu.edu.tr/~gulutas/dif/1.pdf

[17]. H.Bin Zang, C.Yang and X.Mei Quan, (2004), “Image authentication based on digital signature and semi-fragile watermarking.” Journal of Computer and Technology.

Available: https://link.springer.com/article/10.1007/BF02973435

[18]. C.S.Lu and H.Y.Mark Liao, (2003), “Structural digital signature for image authentication: An incidental Distortion Resistant Scheme.” IEEE Transactions on multimedia.

Available: https://www.iis.sinica.edu.tw/papers/lcs/1745-F.pdf

Articles from Conference Proceedings

[19]. M.Ghorbani,M.Firouzmand and A.Faraahi,“DWT-DCT(QCD) based copy-move image forgery detection.” International conference on systems, signals and image processing,2011, pp.1-4. Available: https://ieeexplore.ieee.org/abstract/document/5977368

[20].. Z.Zhou and X.Zhang, “Image splicing detection based on image quality and analysis of variance.” International Conference on education technology and computer (ICETC)2010, pp.242-246.

Available: https://ieeexplore.ieee.org/document/5529692

[21].. P.Sutthiwan,Y.Q.Shi,S.Wei and N.Tian,“Rake transform and edge statistics for image forgery detection.” IEEE international conference on multimedia, 2010, pp.1463-1468.

Available: https://ieeexplore.ieee.org/document/5583264

[22]. Z.Fang,S.Wang and X.Zhang, “Image splicing detection using camera inconsistency.” International Conference on multimedia information networking and security,2009, pp.20-4.

Available: https://ieeexplore.ieee.org/abstract/document/5368456

[23]. W.Lu,W.Sun and J.W.Huang, “Digital image forensics using statistical features and neural network classifiers.” International conference on machine learning and cybernetics,2008, pp.12-15.

Available: https://ieeexplore.ieee.org/document/4620890

[24] Z.Zhang,Y.Ren.X.J.Ping,Z.Y.He and S.Z.Zhang, “A survey on passive blind image forgery by doctor method detection.” International conference on Machine learning and cybernetics,2008, pp.3463-3467. Available: https://ieeexplore.ieee.org/document/4621003

[25]. W.Luo,J.Huang and G.Qiu, “Robust detection of region-duplication forgery in digital images.” International conference on Pattern recognition,2006,pp.746-749.

Available: https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=11159

[26]. Fridrich J, “Robust bit extraction from images.” IEEE international conference on in multimedia computing and systems,1999,pp. 536-540. Available: https://ieeexplore.ieee.org/document/778542