ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

STUDY OF VARIOUS COPY MOVE FORGERY ATTACK DETECTION TECHNIQUES IN DIGITAL IMAGES

Sumandeep Kaur*
* M.Tech Student CSE Department GKU, Talwandi Sabo.

ABSTRACT

In today's era of digital technology, security becomes a prominent issue while transferring data from one place to another place. A large amount of data is passed in form of digital images in various areas like military, security agencies and secured networks etc. With the advancement in technology & editing tools like Photoshop, Corel Draw and other software tools, it is very easy to tamper the images. Image forensics determines the authenticity of the images. Image tampering (manipulation) is also called as image forgery. Copy move forgery is more critical in which one part of the image is copied and pasted into another location of the same image to hide details. It can be a crucial task where images are used as evidence like court, medical department etc. Detection of forgery can be difficult if forger has applied some post processing operations like resizing, filtering, rotation, JPEG compression etc. It is seen that image forgery can results into various security issues and hence an efficient system is required to detect the forgery into images. In this paper, we have discussed the various copy move forgery detection techniques which includes Block based & Key Point based techniques.

KEYWORDS: Copy-move forgery, Image forensics, Block-based methods, Feature-based methods.

INTRODUCTION

The advent in digital world is changing our way in which we store and manipulate the data. Digital images are fastest means of information transfer because of their ease of acquisition and storage. These images can be used as evidence like the images that are shown in TV news can be accepted as evidence for the truthfulness of that news. Though this technology has many advantages, it can also be used for hiding facts and evidences. Today, digital images are manipulated in such a way that it is not possible to detect forgery with naked eyes. The act of illegal manipulating or reproducing document, signature, images or banknotes is called Forgery. Forgery is the process of creating fake images. Forgery is easily possible with the software's like Adobe Photoshop, GIMP, and Corel Paint shop. Some forgers performs the forgery for malicious purpose like to hide important features of an image or to convey some wrong information by changing the content. In this case, integrity and authenticity of image is lost.

Fig 1(a) Original Image ***Fig 1(b) Forged Image (Copy-Move)***

Fig 1(a) on the left side having only one street lamp but in Fig 1(b) on the right side having two street lamps, that is created by using Copy-Move Forgery technique.

Image forgery detection techniques are divided into two categories: - Active approach and Passive approach. In the Active approach, Digital images require some preprocessing like Watermarking, or Digital Signatures etc. Digital Watermarking technique is the process of inserting a digital watermark (a known authentication code) into the image at source side, and then this code is being used for verification of digital information at the time of detection. Watermarks are inseparable from the images. The limitation of Watermarking approach is that it needs to be embedded in image at the time of recording the image before distribution by an authorized person with specialized cameras, but now-a-days most of the cameras are not equipped with the function of embedding watermark. This may also results in degradation of image. Digital Signature approach extracts the unique features of image and encodes them to create digital signatures. These Signatures are used for verification at the detection time.

Passive approach is also called Blind approach which requires no prior information about the image. Image forensics is a passive approach that works on the assumption that these forgeries leave no visual traces; they might alter the statistical properties of the image, referred to as the fingerprints of image that characterizes the life cycle of image from its acquisition to its processing. The manipulation in the image distorts that fingerprints that create inconsistencies in the image. Passive approach applies techniques for the verification of these fingerprints in order to detect tampered region. Passive approach determines the location and amount of forgery in the image. Passive approach has two methods:-

1. Image source identification- This category concerns with the challenges associated with the data source identification. It checks whether the image is computer generated or a natural image and also identifies the device which is used to acquisition of the image.
2. Tampering detection- Image manipulation has become much easier due to availability of digital editing tools that results in complexity of forgery detection. It detects the manipulation of images. Image forgery detection can be manipulated in numerous ways with many Simple operations like affine transforms such as translation, scaling and Compensation operations like colors, contrast adjustments, brightness etc., Suppression operations filtering, compression, noise extraction etc.

Passive approach can be further categorized: -

Pixel-based image forgery detection: Pixel based techniques focuses on the pixels of image and finds the statistical anomalies at the pixel level. These techniques are further categorized: Image Resampling, Image Splicing, Copy-Move forgery.

Format-based image forgery detection: Format based techniques are based on image formats and works mainly in JPEG formats. Format based techniques can detect forgery in the compressed images. These techniques can be divided into three types: JPEG Quantization, JPEG Blocking.

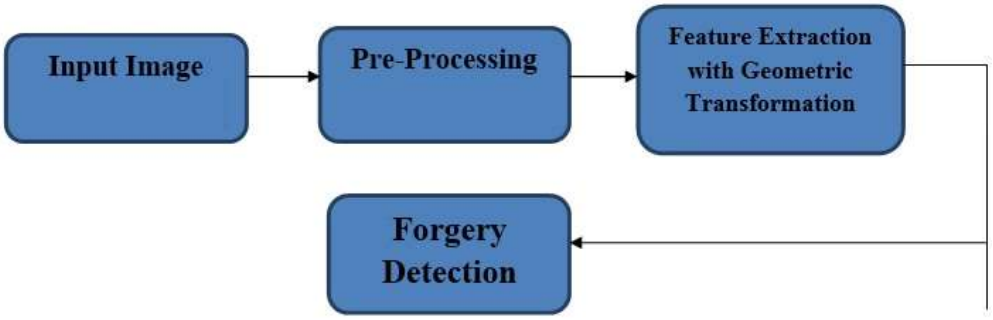
Camera-based image forgery detection: When the image is captured from a digital camera, the image moves from camera sensor to memory. It has to undergo a series of processing steps that includes Quantization, White balancing, Filtering, JPEG compression etc. these techniques can be divided into four categories: Chromatic Aberration, Sensor Noise, Camera Response, Color Filter Array.

Physical environment-based image forgery detection: Consider the creation of an image by splicing together two individual images captured at different places. Here is often difficulty arise to exactly match the lighting effects under each image was originally photographed. These lightening differences can be used as evidence of forgery. Physical environment based techniques works on the basis of lightening environment. These techniques are categorized as: Light Direction 2-D,Light Environment, Light Direction 3-D.

Geometry-based image forgery detection: Geometry based methods make measurement of objects in the real world and their position relative to the camera. Geometry based methods are: Principal Point, Metric Measurements.

GENERAL METHOD FOR FORGERY DETECTION

Copy-Move Image Forgery Detection



EXISTING TECHNIQUES

The Copy-Move forgery detection can be categorized into two methods:-

- Block based Method
- Key point based Methods

Block based Methods:

Block based methods aims to divide the image into overlapping or non-overlapping blocks of equal size rather than identifying the entire forged regions. Then transformation for each block is calculated and a comparison is made in order to detect duplicated regions. The regions of image that are covered under matching blocks are copy-moved regions. Algorithm for block based method is:-

Step 1: Input image & convert it into Grey Scale image. Divide the image into equal sized overlapping or non-overlapping blocks.
Step 2: Compute the feature vector for each block.
Step 3: Blocks are sorted lexicographically based on these features.
Step 4: Match each & every feature vector by searching its approximate nearest neighbor.
Step 5: Forgery Decision is made based on the matched blocks.
These techniques can be classified as:

Moment-based Methods

Under this classification, Copy move forgery is detected by calculating Blur invariant, Hu, Zernike moments among others.

Dimensionality Reduction-based :

This classification includes PCA, SVD, KPCA, PCA-EVD.

Frequency-based Methods:

These methods include DCT, DWT, FMT, PHT, DyWT, QCD, LBP, Curvelet.

Intensity-based Methods:

It includes LUO, BRAVO, LIN, CIRCLE, PCMIFD.

Key Point-based Method:

Keypoint-based methods operate on entire image. Features are extracted only for the keypoints. It increases its computational efficiency. SIFT (scale invariant feature transform) and SURF (SpeededUp Robust Features) methods are used to detect copy-move forgery. General algorithm using SIFT:

Step 1: Image is loaded as input and converted into grey scale image.
Step 2: Then search for SIFT keypoints is made. SIFT features are computed for keypoints.

Step 3: Feature matching based clustering approach is used. Best matching keypoints are clustered in a group and cosine distance between features is calculated.

Step 4: Read the keypoints then comparison of keypoints is made, if a match found between keypoints then draws a line that indicates matched keypoints.

Step 5: Next step is Homographic matrix that tells about the relation between keypoints and provides total matched keypoints.

LITERATURE SURVEY

K.Kiruthika et al.[1] used the keypoint based method SURF(SpeededUp Robust Features) for feature extraction. The g2NN strategy is done for identifying the matched points and hierarchal clustering is done on matched points to reduce false detection rate. TakwaChihaoui et al. [2] proposed a method that automatically detect duplicated regions by identifying local characteristics of the image using SIFT (Scale Invariant Feature Transform) and by using SVD (Singular Value Decomposition) for matching between identical features. This hybrid method is robust to Geometrical Transformations and able to detect with high performance duplicated regions. Sudhakar.K et al. [3] presents an efficient method for copy move forgery detection using SIFT features and used Chan-Vese's Level Set approach to reduce the volume of these features. Multiple forged object detection, high speed, invariant to scale and rotation, robustness and simplicity in implementation are strengths of this method. Lu Liu et al. [4] proposed an improved SIFT based method for copy move detection which combines BFSN (Broad First Search Neighbors) clustering and CFA (Color Filter array) features. BFSN clustering algorithm is used to detect multiple copied areas and to distinguish original regions from tampered regions CFA features are used. This method is efficient on different forgeries and also robust and sensitive. Mohammad FarukhHashmi et al. [5] proposed a method based on DWT (Discrete Wavelet Transform) that is used for dimension reduction and also improves the accuracy of results. It localizes the forgery.

Cao et al. [6] proposed a robust copy-move detection algorithm based on DCT for finding DC coefficients. Irene Amerini et al [7] proposed a novel methodology based on SIFT that detects the copy-move forgery and also recover the Geometric Transformation used to perform cloning. It also deals with multiple cloning. Ghorbani et al. [8] presents DWT-DCT (QCD)-based detection. Authors used DWT and divided the image into sub-bands and then performed DCT-QCD (quantization coefficient decomposition). After sorting lexicographically, shift vector is compared with threshold and forged region is detected. Kang et al. [9] proposed a method for copy-move forgery detection. Authors divided the image into sub blocks and used improved SVD. But it is not successful for noisy images. Lin et al. [10] proposed a method based on improved PCA. PCA is used for finding feature vectors and dimension reduction, after that radix sort is applied on feature vectors to detect forgery. This algorithm is efficient but not works well with compressed and noisy images.

CONCLUSION

This paper represents the various techniques for copy-move forgery detection in digital images. As concluded copy move forgery detection is an important area of image processing for security reasons. A lot of work has been completed for copy move forgery detection for image cloning. An efficient system is required to be developed that can detect the copy move forgery if forged part from an image is compressed, enhanced and or overlapped.

REFERENCES

[1] K.Kiruthika, S.DeviMahalakshmi, K.Vijaylakshmi,"Detecting Multiple Copies of Copy-Move Forgery Based on SURF", International Journal of Innovative Research in Science, Engineering and Technology, ISSN 2319-8753 volume 3, special issue 3, 2014
[2] TakwaChihaoui, Sami Bourouis, KamelHamrouni. "Copy-Move Image Forgery Detection Based on SIFT Descriptors and SVD-Matching", IEEE 1stInternational Conference on Advanced Technologies, Signal and Image Processing, Sousse Tunisiya, 2014
[3] Sudhakar. K, Sandeep V.M, SubhashKulkarni, "Speeding-up SIFT based Copy Move Forgery Detection Using Level Set Approach", IEEE International Conference on Advances in Electronics, Computers and Communications, 2014
[4] Lu Liu, Rongrong Ni, Yao Zhao, Siran Li, "Improved SIFT-based Copy-Move Detection using BFSN Clustering and CFA Features", IEEE Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2014.
[5] MohammadFarukhHashmi, Aaditya R. Hambarde, Avinash G. Keskar, "Copy Move Forgery Detection using DWT and SIFT Features", IEEE 13thInternation Conference on Intelligent Systems Design and applications, 2013
[6] Yanjun Cao, T. Gao, and qunting Yang, "A Robust Detecton algorithm for Copy-Move Forgery in Digital Images", Forensic Int. Volume 214, pp. 33-43, 2012

[7] Irene Amerini, LambertoBallan, Roberto caldelli, Alberto Del Bimbo, Giuseppe Serra, "A SIFT-based Forensic Method for Copy-Move Forgery Attack Detection and Transformation Recovery", IEEE Transactions on Information and Security, vol.6, No.3, September 2011
[8] M.Ghorbani, M.Firouzmand, A.Faraahi, "DWT-DCT (QCD) based Copy-Move Image Forgery Detection", 18th IEEE International Conference on Systems, Signals and image Processing, 2011, pp.1-4
[9] L.Kang, X.-P. Cheng, "Copy-Move Forgery Detection in Digital Image", 3rd International Congress on Image and Signal Processing, IEEE Computer Society,2010, pp. 2419-21
[10] H.-J.Lin, C.W.Wang, Y.-T.Kao,"Fast Copy-Move Forgery Detection", in WESAS Transaction on Signal Processing,2009, pp.188-97
[11] MohdDilshan Ansari, S.P.Ghera, VipinTyagi,"Pixel-based Image Forgery Detection:A Review", IETE Journal of education, Vol 55, No 1, 2014
[12] Ju zhang, Qiugi ruan, yi jin, "Combined SIFT and BI-Coherence Features to Detect Image Forgery", IEEE ICSP2014 Proceedings
[13] Bo Liu and Chi-Man Pun, "A SIFT and Local Features based Integrated Method for Copy-Move Attack Detection in Digital Image", Proceedings of the IEEE International Conference of Information and Automation Yinchuan, China, August 2014
[14] Maryam Jaberi, George Bebis, Muhammad Hussain, Ghulam Muhammad, "Improving the Detection and localization of Duplicated regions in Copy-Move Image Forgery", IEEE,2013
[15] Swapnil H. Kudke, A.D. Gawande, "Copy-Move Attack Forgery Detection by using SIFT", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN:2278-3075, Volume-2, Issue-5, April 2013
[16] Ms.P.G.Gomase, Ms. N.R. Wankhade, "Advanced Digital Image Forgery Detection: A Review", IOSR Journal of Computer Science (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN:2278-8727, PP 80-83, 2014
[17] Salam A.Thajeel, Ghazali Bin Sulong, "State of the Art of Copy-Move Forgery Detection Techniques: A Review", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No. 2, November 2013
[18] Amanpreet Kaur, Richa Sharma, "Copy-Move Forgery Detection using DCT and SIFT", International Journal of Computer applications (0975-8887), Volume 70-No.7, May 2013
[19] Barnali Sarma, Gypsy Nandi, "A Study on Digital Image Forgery Detection", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 11, November 2014
[20] Amanpreet Kaur, Richa Sharma, "Optimization of Copy-Move Forgery Detection Technique", International Journal of advanced Research in Computer Science and software Engineering, Volume 3, Issue 4, April 2013
[21] Tushant A. Kohale, P.R. Lakhe, S.D. Chede, "Detection of Postoperated Copy Move Image Forged by Integrating Block Based and Feature based Method", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, January 2014
[22] Dhanshri P. Patil, "Forensic Technique for Detecting Image Tampering using statistical Intrinsic Fingerprints: A Survey", International Journal of Scientific Engineering and Technology, Volume No. 3, Issue No. 7, pp: 919-920, ISSN: 2277-1581, July 2014
[23] Resmi Sekhar, 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