JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

REVIEW: FORGERY DETECTION IN IMAGE

[1] NAYANASHREE N, [3] NANDITHA R. [4] NEHA RANA. [5] KAVYA S, [2] SUDHA M S

[1345] STUDENT, [2] ASSOCIATE PROFESSOR
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING,
CAMBRIDGE INSTITUTE OF TECHNOLOGY, KR PURAM, BENGALURU-36, INDIA.

ABSTRACT:

Regarding with the development of digital picture processing software and editing tools has made it remarkably easy to exploit digital images. So, definitely, the need for reliable image falsification detection has turned into paramount. Trust me! Such detection is essential in various fields, including forgery investigations and legal proceedings. Pixel-based image falsification detection aims to authenticate, like, digital images without any earlier grasp of the original image. So, like, image tampering can take multiple forms, such as splicing, copy-move, and resampling, which is like resizing, rotating, stretching, and the addition or removal of objects or whatever. In this paper. We will explore various pixel-based techniques primarily focused on copy-move and bind detection.

Keywords: Digital forensics, copy-move forgery, duplication forgery detection, forgery detection

Introduction:

The latest advancements in imaging technologies have provided forgers with the necessary tools to manipulate digital images by adding deceptive elements without leaving any noticeable traces. Many researchers have suggested the establishment of image authenticity as a means of detecting these fraudulent activities, which can be prevalent in various kinds of fields such as criminal investigation, medical imaging, journalism, intelligence services, and surveillance systems. Consequently, techniques for detecting digital forgeries have existed to address this issue, serving as an essential aspect of image processing.

Classification of Digital Forgery Techniques

Different research works have been managed in different domains to enhance existing techniques in the recognition of copy-moving forgery, which includes techniques involving the hiding, addition, or alteration of specific areas in an image. The main types of forgery techniques in digital pictures can be varieties into three groups: Copy-Paste (splice), Image retouching, and Copy-Move (Cloning). For instance, the retouching technique involves manipulating the digital photos by modifying their characteristics while ensuring that the content remains unnoticeably altered. Otherwise, image clustering utilizes new images by adding additional images to generate a tampered version, enabling forgers to hide or modify the content of the picture. Furthermore, image cloning entails copying a specific part of a picture and relocating it to another area within the same image, allowing for the concealment or duplication of certain elements.

Current Efforts in Image Falsification Detection:

The development of reliable methods for the detection of picture falsification has collected significant attention from researchers. Existing detection methods in literature can be classified as either active or passive. Active detection methods, such as watermarking, involve embedding additional details within the image to describe digital tampering, such as names, dates, or signatures. Otherwise, the passive

technique aims to identify forgeries or duplicated objects in images without considering the information from the original images. The main reason for this method is to demonstrate the possibility of detecting falsification without relying on the appearance of original image watermarks.

LITERATURE SURVEY:

The literature survey conducted by Sudha M Set all focuses on digital image copyright protection and access control. It also touches upon the idea of steganography, which refers to the privacy of information in surveillance. Various techniques like security links, blotters, digital signatures, and spectrum communication are used in steganography. Additionally, the survey highlights the application of steganography as a commercial use of steganography.

Information Falsification in Digital Images Sudha M Set all emphasize the importance of detecting and restoring falsified information in digital picture documents during the communication process. This is particularly crucial for protecting important documents such as sweep investigate, gold bond proof, and signed documents. The detection and repair technique for tamper detection is essential in safeguarding these documents.

Precise and Derived Match Techniques for Healthy Detection Jessica Fridrich, David Soukal, and Jan Lukas et all propose two techniques for healthy detection in images. The first technique relies on a precise match, while the second technique is a kind of derived match. The algorithms used involve identifying precise parts within the image through pixel representation of squares. The derived match technique differs from the precise match technique in that it does not order and match the blocks but instead uses robust representation involving trigonometric function transforms coefficients. Despite being efficient. The below methods may not produce highly accurate matching results.

PCA-based Algorithm for Image Block Analysis

Alin C Popescu and Hany Farid et all present an algorithm predicated on Principal Component Analysis (PCA) for analyzing small image blocks. This algorithm provides a reduced dimensional represent a particular is able of predicting slight changes in the photo due to noise.

Actively and Passively Techniques for Image Falsification Detection:

Ferreira, W. D., Ferreira, C. B., da Cruz Júnior, G., and Soares et all categorize image forgery detection methods into two classes: Active and Passive techniques. Active techniques require prior knowledge of elements associated with the original image, such as watermarking or steganographic data. On the other hand, submissive techniques can determine image authenticity without relying on previous information regarding the original image.

Reproduction Pass: Image Falsification Detection form on Ripple Technique:

Saiqa Khan and Arun Kulkarni et all propose a reproduction-pass Image falsification detection method based on the ripple technique. This technique involves using the ripple transform for compression and similarity checking. The detection process consists of two stages: detecting the reference and then matching found on the low-level ripple transform. but this method may not accurately detect forgery when the duplicated image undergoes rotation and scaling.

Key Point-based Technique for Image Forgery Detection:

Xinyi Pan and SiweiLyu et all introduce a key point-based technique for image forgery detection. This technique involves matching Scale Invariant Feature Transform (SIFT) key points and identifying all pixels within the corresponding areas. The technique demonstrates reliable performance in detecting different methods of robust forgery, although it may not be accurate in regions with few visible structures.

FORGERY DETECTION:

Falsification Detecting methods have become increasingly intricate to combat the latest methods of forgery. The emergence of digital editing tools has made alteration and manipulation significantly easier, thereby presenting a complex and serious problem for Falsification detecting [23]. Various simple operations, like affine transforms (e.g., translation, scaling), compensation operations (e.g., brightness, color, contrast adjustments), and suppression

operations (e.g., noise extraction, filtering, compression), can work for photo Forgery Detection [9]. Additionally, more complex operations including compositing, blending, matting, cropping, and photomontage can cause visually undetectable artifacts in a picture [24]. As a result, the automatic and scientific detection of forged images poses a significant challenge for researchers, holding for all types of hypermedia contentment as well.

Block-based methods:

Several techniques for identifying copy-move Falsification are based on block-based methods. Instead of trying to detect the entire forged region, these techniques split up the image into tiny creases or non-overlapping blocks. By comparing these blocks, it becomes possible to identify which blocks are matched and determine the copied and Forgery regions. These techniques can be categorized as follows:

1. **Moment-based (BLUR, HU, and ZERNIKE)**

Mahdian and Saic [28] utilized blur moment invariants to represent image regions. These invariants are unaffected by blur degradation and add-on crash. This process begins with preprocessing the images by tiling them into blocks of a particular area. Each block is represented by blur invariants, Resultant of length 72. These vectors are further normalized to enhance duplication detection. Principal component transformation (PCT) is applied to reduce the capacity of the point vectors. The similarity study of the blocks is conducted using a k-d tree representation. By setting a certain threshold value, Similar blocks are identified and verified by evaluating their non-identical neighborhoods. This method effectively detects copy-move falsification in photos with duplicated regions and changed contrast values. However, it does have a tendency for false alarms and a relatively high computation time.

Wang, Liu, Zhang, Dai, and Wang [16] developed an algorithm using Hu moments for efficient and strong copy-move forgery detection. To reduce dimensionality, they employed a Gaussian pyramid to split the photo into fixed-sized overlapping blocks. Hu moments were then applied to these blocks to calculate eigenvalues. Following lexicographic sorting, an area threshold was chosen to minimize false Detection. Mathematical Morphologic Techniques were owned for matching blocks. This algorithm can Detect copy-move Falsification even after various post-processing techniques, such as blurring or lossy JPEG cropping have been applied.

2. **Dimensionality reduction-based (PCA, SVD, KPCA, and PCA -EVD)**

Popescu and Farid [30] successfully detected copy-move forgery by applying PCA (Principal Component Analysis). They divided the given image into small blocks using a moving window and recorded the Pixel cost for all blocks in an array. Lexicographic sorting of this array helped identify a kind of approach in the matrix rows, leading to the spotting of forged regions. In their robust match method, the blocks were represented by quantized DCT coefficients with a chosen Q-factor. The Sorted model was then worn for matching. This approach effectively reduces false positives by considering mutual pairs. However, it struggles to differentiate large identical textures in natural images.

A method proposed by Bashar, Noda, Ohnishi, and Mori [32] utilizes Discrete Wave Transform (DWT) and the Kernel Principal Component Analysis (KPCA) for copy-move Falsified Detection. The photo is split into minute blocks, and KPCA-based vectors and DWT vectors are planned for every block. These vectors are then kind Lexicographic and used to find similar points and calculate offset frequencies. The introduction of a value for offset frequency helps avoid false detections. Additionally, a labeling technique and geometric transformation are employed to detect flip and rotation forgeries. This algorithm outperforms conventional PCA approaches and can also detect forgeries with JPEG conversion.

3. **Intensity-based (LUO, BRAVO, LIN, CIRCLE, and PCMIFD)**

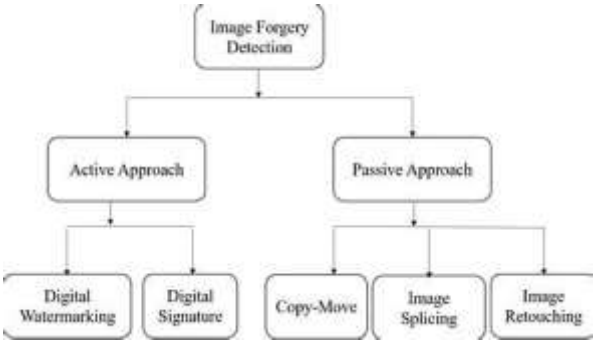
Luo, Huang, and Qiu put forward a method for copy-move faking Detection based on intensities. By resolving the images into overlapping blocks, they computed a block characteristic vector for every slab using the Additive White Gaussian Noise (AWGN) operation. These vectors were lexicographically sorted, and a shift vector method was worn to determine which pairs of related block attribute vectors represented duplicated regions. A definite value of the shift vector was set, and blocks were considered equal when shift vector of a pair passed this value. The highest occurring shift vector determined the threshold for discarding pairs with

significantly different shift vectors. This algorithm has a partially low computational complication and robustness against postprocessing operations. However, it performs best when the forged regions are larger than the lump size and struggles with highly distorted images and large smooth regions. Wang, Liu, Li, Dai, and Wang [36] employed the Gaussian pyramid method to bring down the dimensions of the images. For circle blocks, they calculated four features that were lexicographically sorted. By adjusting the threshold value, matching feature vectors for copy-move forgeries were found successfully. The method was tested on tampered images subjected to various postprocessing methods, such as blurring, lossy JPEG compression, and rotation. The efficiency of the detecting techniques was improved to narrow down the search space for block matching.

4. Frequency-based (DCT, DWT, FMT, PHT, DyWT, QCD, LBP, and Curvelet)

Fridrich, Soukal, and Lukáš [38] utilized Discrete Cosine Transform (DCT) coefficients for finding copy-move forgery. They divided the images into blocks using a window and recorded pixel values for each and every block. Lexicographic sorting of these pixel values allowed for the spotting of similar entries in the matrix rows, ultimately revealing the found regions. To handle false positives, a robust match method was employed using quantized DCT coefficients. However, this method struggles to distinguish between large identical textures in natural images.

Muhammad, Hussain, Khawaji, and Bebis [14] explained the Robust method for detecting copy-move forgery using Dyadic Wavelet Transform (DWT). This method involves extracting low-frequency and high-frequency components from the image, followed by matching using a similarity measure. DyWT, being shift-invariant, is preferred over Dew, which lacks shift-invariance. The authors decomposed the image using low-pass and high-pass filters.



ACTIVE APPROACH:

This technique involves the digital icon that requires pre-processing to generate the watermark and embed or sign the images. However, this can limit their application. Mechanized watermarking [4] and stamps are lively assertion systems, as something is implanted into photos once, they are obtained. We can detect if the photo is altered by the inability to remove the original content from the received image. Watermarking is a procedure for lively intrusion disclosure, as a certification form is embedded into the photo, but most existing imaging devices do not include any watermarking or verification module, which is necessary for dynamic security. This method is used for authenticity verification, and if an error is found with the form, then the picture is altered, and a reverse analysis over the frame is conducted to identify the modified space of the photo.

PASSIVE APPROACH:

Image Falsification Potting using JPEG Compression Properties:

JPEG is the most of all popular and most popular compressing technique which has been found in a variation of approach. Many digital cameras export JPEG file formats to recognize whether a picture is in bitmap formats that have been advanced JPEG compact or not it is a major issue for some image organize applications and it will play a major role in image altering detection.

Fan and Queiroz (2003) built a method decided regardless if a picture has been earlier JPEG compressed and estimated. Photographic images and Photorealistic Computer Graphics images classification.

As we know Computer Generated image (CG) technologies hastily develop, advanced graphics rendering programs that can create exceptionally

photorealistic images. These images can be formed that are hard to recognize vividly from pictorial images. As the depiction technology evolves, photorealistic images can be modeled and rendered easily. One of the challenges and pressing issues is to differentiate between photo-realistic computer-generated (PRCG) pictures from Genuine(photographic) photos.

Projective Geometry:

Photographs sometimes have areas that are combined, making it a challenge to maintain the image's correct perspective. This way it can be tricky to ensure that the composited regions blend seamlessly with the balance of the image. Subsequently, it is not uncommon for the pursuit of tampering to be present in these images.

Johnson and Farid (2006) proposed three techniques that can be old to guess the transformation of a plane under perspective projection. These methods are designed to rectify planar surfaces to be front-parallel, making it easier to accurately assess and analyze the resemblance of the image. The best part of this ability only requires a single image, which makes the process more efficient and accessible.

Image Processing Operations:

Image processing is a vital aspect of concealing defines the tampering in images. Various image processing operations are often active to the images to achieve this objective. Identification of these efforts becomes crucial in detecting forgeries.

Lukas (2000) has popped up a method that involves the utilization of convolutional filtering and spectral operations to detect cover-ups in digital images. This technique, despite its complexity, has proven to be effective in uncovering tampering.

Aveibas (2004) has presented an alternative approach that enables the perception between tampered images and their originals. This method relies on content-independent distortion measurement. It provides insights into the accuracy of the profile and the identification of manipulated content.

STUDY ON METHODS:

Different image copy-move forgery detection techniques are considered and analyzed for the period range between (2017-2020) in this section. A recent study has come up with a method for detecting interference based on a multitexture description [4]. Local Phase Quantization (LPQ), Binary Statistical Image Feature, and Binary Gabor Patterns are the various texture descriptors considered. Using the image decomposition Steerable Pyramid Transform (SPT), the method captures such slight texture variation at various scales and orientations. After SPT decomposition, the different texture descriptor extracted from each sub band image is combined to form the multi-texture representation. Then, to generate a compact representation, the relief feature selection method applies to this high-dimensional multi-texture representation. This lightweight, multitexture representation is categorized using the classifier Random Forest.

Chun-Su Park & Joon Yeon Choeh introduced a quick method that is up to recognize forgery with multiple geometric transformations such as region rotation, resizing, deformation, and reflection [6]. SIFT is used to extract the key points and their descriptors to recognize copy-move forgery. The suggested CMFD method has a solid theoretical background, which has a higher performance than the present SIFT-based algorithms. This method has better processing time.

Mohamed Abdel-Basset et al. suggested a technique that could detect the exploitation of this kind and identify the duplicated areas [7]. SIFT is found in that strategy. It is a well-known robust technique capable of detecting and matching features that belong to duplicate regions. These matched features are placed under the umbrella of a 2-level clustering strategy to ensure that features are later used to help in the geometric modifications of the duplicate areas belonging to particular clusters representing the included section in the image.

Chengyu Wang et all proposed to use two techniques accelerated-KAZE (A-KAZE) and speed-up robust features (SURF) to detect a copy-move forgery image [9]. Only one of them is the main drawbacks of key points techniques is to get enough points in smooth regions. In the proposed method, the response thresholds for the feature detection stage A-KAZE and SURF are set at small values to mitigate this defect. Also, a new map of the correlation coefficient

is shown, in which bounding the duplicated regions, integrating filtering, and mathematical morphology.

Conclusion:

In the current proposal, the presentation and explanation of the concept of forgery are introduced and we focus a lot on copy-move image Forgery detecting. Passive methods analyze Image properties without relying on additional information. Techniques like noise analysis. sensor pattern noise and block artifact detection help identify inconsistencies. Active methods involve embedding information or using watermarks. Collaboration between researchers, industry, and policymakers is essential to stay ahead of emerging threats.

References:

Sudha, M. S., and T. C. Thanuja. "Digital Image Authentication (Dia)-A Survey." Proceedings of IRF International Conference, Bangalore 23rd March 2014. 2014.

Sudha, M. S., and T. C. Thanuja. "Randomly tampered image detection and self-recovery for a text document using Shamir secret sharing." 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). IEEE, 2016.

Ferreira, W. D., Ferreira, C. B., da Cruz Júnior, G., & Soares, F. (2020). A review of digital image in forensics. Computers & Electrical Engineering, 85, 106685.

Thajeel, Salam A., and Ghazali Bin Sulong. "State of the art of copy-move forgery detection techniques: a review." International Journal of Computer Science Issues (IJCSI) 10.6 (2013): 174.

Pan, X. Z., & Wang, H. M. (2012). The Detection Method of Image Regional Forgery Based DWT and 2DIMPCA. Advanced Materials Research, 532, 692-696.

Shivakumar, B., and S. Santhosh Baboo. "Automated forensic method for copy-move forgery detection based on Harris interest points and SIFT descriptors." International Journal of Computer Applications 27.3 (2011): 9-17.

Yao, Heng, et al. "Detecting copy-move forgery using non-negative matrix factorization." 2011 Third International Conference on Multimedia Information Networking and Security. IEEE, 2011.).

Pujari, Vidya S., and Mandar Sohani. "A Comparative Analysis on Copy Move Forgery Detection in Spatial Domain Method Using Lexicographic and Non-Lexicographic techniques." IJECCE 3.1 (2012): 136-139.

Chen, Likai, et al. "Region duplication detection based on Harris corner points and step sector statistics." Journal of Visual Communication and Image Representation 24.3 (2013): 244-254.

XU, Mei-hong LIU Wei-hong. "Detection of copy-move forgery image based on fractal and statistics." Journal of Computer Applications 31.08 (2011): 2236.

Yadav, Preeti, Yogesh Rathore, and Aarti Yadu. "DWT based copy-move image forgery detection." International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) 1.5 (2012): 56-58.

Pujari, Vidya S., and Mandar Sohani. "A Comparative Analysis on Copy Move Forgery Detection in Spatial Domain Method Using Lexicographic and Non-Lexicographic techniques." IJECCE 3.1 (2012): 136-139.

Ansari, Mohd Dilshad, Satya Prakash Ghrera, and Vipin Tyagi. "Pixel-based image forgery detection: A review." IETE Journal of education 55.1 (2014): 40-46.

Gill, Navpreet Kaur, Ruhi Garg, and Er Amit Doegar. "A review paper on digital image forgery detection techniques." 2017 8th international conference on computing, communication, and networking technologies (ICCCNT). IEEE, 2017.

Abd Warif, N. B., Wahab, A. W. A., Idris, M. Y. I., Ramli, R., Salleh, R., Shamshirband, S., & Choo, K. K. R. (2016). Copy-move forgery detection: survey, challenges and future directions. Journal of Network and Computer Applications, 75, 259-278.

Thajeel, Salam A., and Ghazali Bin Sulong. "State of the art of copy-move forgery detection techniques: a review." International Journal of Computer Science Issues (IJCSI) 10.6 (2013): 174.

Mehrjardi, Fatemeh Zare, et al. "A survey on deep learning-based image forgery detection." Pattern Recognition (2023): 109778.

Lukas, Jan, Jessica Fridrich, and Miroslav Goljan. "Digital camera identification from sensor pattern noise." IEEE Transactions on Information Forensics and Security 1.2 (2006): 205-214.

Kumar, Sunil, and P. K. Das. "Copy-move forgery detection in digital images: progress and challenges." International Journal on Computer Science and Engineering 3.2 (2011): 652-663.

Khan, S., & Kulkarni, A. (2010, December). Robust method for detection of copy-move forgery in digital images. In 2010 International Conference on Signal and Image Processing (pp. 69-73). IEEE.

Pan, Xunyu, and Siwei Lyu. "Region duplication detection using image feature matching." IEEE Transactions on Information Forensics and Security 5.4 (2010): 857-867.