International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8, Issue-2S3, July 2019

Digital Image Forgery Detection

S.Prayla Shyry, Saranya Meka, Mahitha Moganti

ABSTRACT--- With the growing challenges in authenticity and integrity of images, image manipulation has crumbled assurance over digital image. The major motivation of the forgery in image is manipulating the image in such a way that it cannot be distinguished to the naked eye. Image manipulation has increased the demand to assess the trustworthiness of digital images when used in crime investigation, as witness of law and for surveillance purposes. In this paper, various types of image forgery and detection techniques have been explained. Initially different kinds of forgery attacks are categorized and summary of passive approach is discussed.

Index Terms: Digital Image; Forgery; Forgery detection; Copy move forgery; Tampering

I. INTRODUCTION

Forgery is an illegal means of manipulating images or documents without prior access. Images are tampered for different reasons either to create false evidence or to earn money in an illegal way. An pictorial representation of image conveys much better idea than the words of human. Due to the progression in digital technology, images are proceesed using several tools like Adobe Photoshop, GIMP and Corel Paint Shop and they ended up with a threat for the authenticity of digital images. Generally, image manipulations are of two types a) Allowed manipulation b) Malignant manipulation.

Fig 1.Original Image Fig 1 Fake Image

Allowed or incidental manipulations are the ones which never alters the semantic sense of information and are acceptable by any authentication system. The edits made should be very minor and subtle. Manipulation of images is generally allowed when correcting the color, tuning the brightness and contrast of the photo, fiiting a layout using cropping a frame, reducing the noise like dust ,dirt or scratches in the photo. Combining certain parts of whole image or leaving out certain parts of an image is acceptable unless they are mentioned and differentiated preferable by using boxes that portray the different parts of the image.

Semantic sense is really changed in Malignant manipulation and this fashion should not be repeated. Moreover it never performs adding, moving or removing objects within the frame, changing the color other than to restore what the picture actually looks like, to alter its interpretation, cropping a frame in order, flopping an image either left or right reversal, and lastly painting a photograph in other than its true orientation. Image forgery has two flavours namely Active and passive based approach. Non-blind/intrusive methods are commonly referred to as Active methods and it need major processed data to be embedded in the original image during the recording.

Due to this necessitous, active approaches have restricted scope. Digital watermarking and digital signatures are some of the examples. Watermarking involves injecting a watermark which is used for the authenticity of the digital image which is indivisible from the image. On the other hand, Passive methods are the non-intrusive/blind methods and it never needs any prior information to include in the digital image. A digital image can be tampered by different attacks like resizing, adition of noise, blurring, rotation, scaling compressing, image splicing, copy-move and many more.

II. LITERATURE WORK

Toqeer et al detected the copy-move forgery attack, in which the images are splitted in overlapping square blocks and for the block representations DCT components are adopted. Reduced dimensional nature of the feature space is required to improve the efficiency of image matching and so Gaussian RBF Kernel PCA is implemented. The proposed method is compared with the traditional methods and their results revealed best credibility of images with better efficiency.

Anita Sahani et al inroduced a method for image forgery detection which plays the role for replacement, insertion and removal of objects.SVM classifier which has a comparable utilitarian shape like neural systems is utilized. At first Image, the values of surface and pixel are extracted and after analyzation hash values are determined.This strategy comprises of two stages namely preparing or training stage and testing stage. SVM classifies both original and fake images and the information is secured using RSA algorithm.

Revised Manuscript Received on July 10, 2019.

S.Prayla Shyry, CSE, Sathyabama Institute of Science and technology,Chennai,Tamil Nadu. India.

Saranya Meka, CSE, Sathyabama Institute of Science and technology Chennai,Tamil Nadu. India.

Mahitha Moganthi, CSE, Sathyabama Institute of Science and technology ,Chennai,Tamil Nadu, India.

Retrieval Number: B11210782S319/19©BEIESP
DOI : 10.35940/ijrte.B1121.0782S319

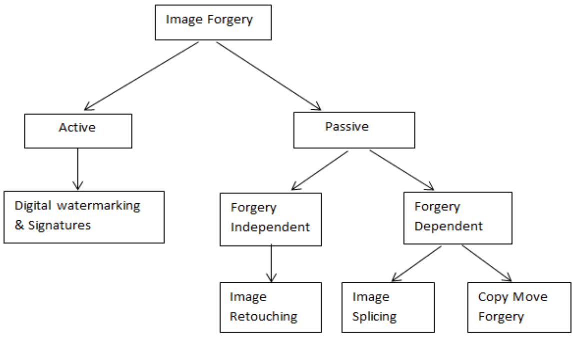
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Shivani et al developed a technique of SIFT algorithm which is applied to mark the objects in the image. They used the SIFT algorithm where a whole image is scanned and from the scanned image objects are marked. The properties of the marked object are accessed and objects which have similar properties are classified into a group and other are into second. To classify the similar type of objects techniques like block-based & Key Point based technique, shift key point can be used.

Jian et al proposed a novel forgery detection schemes using copy-move At first, the test picture is splitted into semantic free fixes of preceding key point extraction. Accordingly, a match between patches can identify the duplicate move locales. The coordinating procedure comprises of two phases. At first, the sets of patches(suspicious) contains duplicate move fraud locales and generally evaluated a relative change grid. Expectation-Maximization-based calculation is intended to refine the evaluated network and to affirm the presence of duplicate move fabrication. Trial results on general society databases demonstrate the upstanding execution of the proposed plan by means of contrasting it and the cutting edge plans.

Mohammad et al integrated Hidden Markov Model (HMM) and Support Vector Machine(SVM) Classifier for image forgery authentication. They consolidated discrete cosine change (DCT) measurements, LBP highlights with curvelet insights and Gabor change of the pictures to speak to a picture in the changed area. To verify the technique CASIA image dataset is used which contains seven thousand authentic and tampered images. To perform training and testing they divided the dataset into two halves. Changed pictures are utilized to prepare the Hidden Markov display as HMM can separate probabilistic state data from a huge measurable model.

III. CATEGORIZATION OF IMAGE FORGERY TECHNIQUES



IV. ACTIVE APPROACH

In an active approach, the first phase consists of pre-processing technique that is watermark injecting. Watermarking makes active tampering detection, which involves injecting a special pattern into the owner (source) image so that piece of information gets authorized. This special pattern can be further used to notify the user either the image is tampered or not. But today large portion of the imaging gadgets don't contain any watermarking or mark module.

Digital signatures are part of an active approach in which some bit patterns are embedded in the digital image to avoid image manipulation. Dynamic picture validation utilizes a realized verification code while picture gaining or sending which is infused into the picture or sent alongside it for surveying its legitimacy or honesty at recipients side. It is varied from exemplary information validation. Sensitivity and robustness are two primary needs of active image authentication. Digital watermarking and digital signatures are the main active image authentication approaches.

V. PASSIVE APPROACH

Though there are different traditional methods which can detect forgery in unique way, there is no exact method that can treat all these cases. The stream of latent altering identification manages breaking down the crude picture dependent on various measurements and semantics of picture substance to restrict altering of the picture. Neither develop is infused in the picture and nor related with it for security, as like dynamic methodologies and consequently this technique is otherwise called crude picture investigation. The confinement of altering is just relying upon picture highlight measurements. Along these lines, calculations and strategies for location and limitation of picture dependent on aloof recognition change contingent on the kind of security develop utilized. In any case, uninvolved altering location is usually goal to the limitation of altering on crude picture.

VI. TYPES OF PASSIVE APPROACH

I. Image splicing

Image splicing is the method of making a composite image by cropping and combining two or more images .Unlike image retouching this technique is more aggressive for creating forgery images. A number of sharp transformations such as edges, lines, and corners can be introduced in a spliced image. Examples include the use of fake images by several infamous news reporting cases. Image splicing is used with later post-processing techniques like smoothing boundaries of fragments or even without post-processing.

II. Image retouching

Image retouching is adding or removing something from the image for enhancing features of an image. This technique is applicable for used for aesthetic, commercial users and it degrades the image features.Generally, it is popular among magazine photo editors, where they try to make an image more attractive by enhancing some features. Compared to all available forgery techniques Image Retouching is considered as less harmful. Removing blemishes on a picture of a model would be a great example of image Retouching.

III .Copy-Move attack

Copy Move copies and paste a specific portion of the image. Since the copied region represents the same image,the dynamic range and color remains same. In this technique, we add or remove information to cover a part of the image. Some image or text is masked in original image.

A. SVM Classifier

SVM classifier detects forgery in images by calculating the hash values for extracted features. In the training phase, the RSAis used in testing phase to ensure the authenticity of person. Image classification, bioinformatics, bio-sequence analysis, hand-writing recognition, and many more complex real world problems can be attained through SVM. SVM works in two phases –the training phase and testing phase.

Initially, a database is created with a larger number of jpg or jpeg images and trained in the training phase. These images can be of any size and can be captured through a camera or downloaded from the internet. RSA key is fixed in the database after training images. Authorization is provided by entering the same RSA key provided during the training phase. These images are further converted from RGB to grayscale which the noise is removed by applying Median filter.

Image enhancement techniques are applied which include contrast manipulation & gray level, interpolation and magnification, pseudo coloring, edge crisping and sharpening, filtering, noise reduction, etc. Feature Extraction is done using image analysis, pixel value analysis, and texture analysis and hash values are calculated correspondingly. Decision boundaries are defined by SVM classification whereas no algorithms have nice theoritical approach.

VII. B. NAÏVE BAYES CLASSIFIER

Naïve Bayes is used as an image classifier due to its effectiveness for larger datasets. It assumes that there is an independent relation between the presences of a feature in a class is independent of the presence of any other feature. Bayes rule is applied to the image for the classification. Bayes' theorem follows simply from the principles of conditional probability.

Posterior probability $P(C_K|x)$ is the updated probability of an event occurring after taking into consideration new information. Before collecting the empirical data, a prior probability is based on established knowledge.

$$\mathbf{A(CK|x) = \frac{A(ck)p(x|ck)}{A(x)}} \qquad \mathbf{(1)}$$

Where $A(C_K|x)$ – Posterior
$A(c_k)p(x|c_k)$ - prior * likelihood
A(x) - Evidence

VIII. COPY MOVE FORGERY DETECTION USING BLOCK BASED

In this method, Blocks of images are used for analyzing the forgery. Images are to divided into overlapping or non-overlapping blocks than analysing the entire image at the same time.

IX. ALGORITHM & RESULTS

i. Images are divided into small overlapping or either non-overlapping blocks
ii. Extract the features using traditional techniques
iii. Extracted feature values corresponding to each blockare stored in matrix.
iv. Apply sorting techniques to get similar features that lie in nearness.
v. Introduce shift vector concept to find blocks with similar shifting
vi. Use the counter vector to count the occurrence same shifting blocks and set the counter to 1
vii. Similar regions are identified with the help of threshold value

Above steps are used to identify the forged blocks in an image. Block-based techniques can be further divided into

a.Copy move forgery detection using Key point based approach

Key-point based methods can distinguish foreground to background. Unlike block based approach it forms descriptors from specific areas. Using SURF(Speed Up Robust Features),SIFT(Scale in-variant Feature Transform),GLOH,ORB (Oriented FAST (Features from Accelerated Segment Test) etc., detection algorithms on descriptors yields better results. In image, regions with high entropy are collected to form feature vectors which follow a series of steps including greyscale conversion, image subdivision. Matching is done on similar feature vectors forming a cluster into large areas which reports a forgery. The resultant output is more efficient that block based method. Post-processing may be done such as filtering, edge detection etc.

b. Passive based Image forgery detection

In the passive approach, the digital signature is not used for the purpose of authentication. Assumptions are made while tapering the image that digital forensics may not leave any visual clue. It alters the underlying statistics of the image. Passive based Image forgery detection can be done using any of these techniques:

a) Pixel based technique
b) Format based technique
c) Camera based technique
d) Physically based technique
e) Geometric based technique

X. CONCLUSION AND FUTURE WORK

We conclude our study on image forgery techniques .Study of different image forgery techniques has been done elaborately with pros and cons. This paper reviewed various traditional techniques which are been used. Though accuracy of detecting forgery in image using traditional methods is attained to certain level, improvement in existing techniques is required for better accuracy. Combination of machine learning algorithms could be a better option to yield accuracy. In future, SVM(Support Vector Classifier) can be used along with other machine learning techniques for better results.

REFERENCES

1. A.C. Popscu, and H.Farid, "Statistical Tools for Digital Forensics" ,in Proc.The 6th international workshop on information hiding ,Toronto, Canada 2004.
2. Shivani Thakur, RamanpreetKaur, Dr. Raman Chadha,JasmeetKaur, "A Review Paper on Image Forgery Detection In Image Processing", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. I (Jul.-Aug. 2016), PP 86-89
3. DevanshiChauhan, DipaliKasat, SanjeevJain, VilasThakare, "Survery on KeyPoint based Copymove Forgery Detection Methods on Images", science direct volume 85 2016.
4. Ali Qureshi, M., and M. Deriche. "A review on copy move image forgery detection techniques." IEEE, 2014..
5. Qazi, Tanzeela. "Survey on blind image forgery detection."IET, 2013.
6. M. Qiao, A. Sung, Q. Liu and B. Ribeiro, "A novel approach for detection of copy-move forgery," Fifth International Conference on ADVCOMP (Advanced Engineering Computing and Applications in Sciences, 2011.
7. Gajanan K. Birajdar, Vijay H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10, no.3, 2013, pp. 226-245.
8. GagandeepKaur, Manoj Kumar, "Study Of Various Copy Move Forgery Attack Detection In Digital Images", International Journal Of Research In Computer Applications And Robotics, Vol.3 Issue 9, Pg.: 30-34 September 2015
9. Rohini.A.Maind, AlkaKhade, D.K.Chitre, "Image Copy Move Forgery Detection Using Block Representing Method", International Journal Of Soft Computing And Engineering (Ijsce) Issn: 2231-2307, Volume-4, Issue-2, May 2014.
10. R.C. Gonzalez, R.E. Woods, "Digital Image Processing", 2nd edition, Addison- Wesley, 2003.
11. 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
12. BarnaliSarma, 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
13. ManpreetKaur, 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
14. J. Fridrich, "Methods for "Methods for Tamper Detection in Digital Images", Proc. ACMWorkshop on Multimedia and Security, Orlando, FL, October 30−31, 1999, pp. 19−23.
15. S. Saic, J. Flusser, B. Zitová, and J. Lukáš, "Methods for Detection of AdditionalManipulations with Digital Images", Research Report, Project RN19992001003"Detection of Deliberate Changes in Digital Images", ÚTIA AV ČR, Prague, December1999 (partially in Czech).

XI. AUTHORS PROFILE

Dr S.Prayla Shyry is presently working as Professor in Faculty of Computing, Sathyabama Institute of Science and Technology, Chennai. Her areas of interest include Network security, Overlay networks. She has 14years of experience in teaching. She has published more than 45 research papers in International/National conferences and International/National Journals. She has actively participated as session chair person, member, organizing committee in various International and National conferences. She has also received best paper Award for her presentation in National conference.

Saranya Meka is doing her final year year in the department of Computer Science and Engineering, Sathyabama Institute of science and Technology.She has published 4 papers in international conferences and journals

Mahitha Moganti is doing her final year year in the department of Computer Science and Engineering, Sathyabama Institute of science and Technology.She has published 4 papers in international conferences and journals.