Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Detection of Image Forgery

Shubham Sharma[1], Sudeeksha Verma[2], Swapnil Srivastava[3]
Student, Department of Computer Science and Engineering,
PSIT College of Engineering Kanpur, India

***Abstract*:- Digital Image Forgery can be done by deceiving the digital image to mask some meaningful or important data of the image. It is usually difficult to spot out the manipulated region of the original image. To sustain the uprightness and legitimacy of the image, the detection of forgery in the image is mandating. Acclimation of the modern way of life and advancement in photography gadgetry has made exploitation of digital image easy with the help of image editing software. Therefore, it is crucial to detect such image forgery operations in the images. The image forgery detection can be done based on object removal, object addition, unusual size modifications in the image. Images are one of the powerful media for communication. In this paper, a survey of different types of forgery and digital image forgery detection has been focused.**

Keywords: Cloning, Splicing, Retouching, Morphing, Copy-Move Forgery

Figure 2: Example of the copy-move forgery where object is been copied in the same image but in the different position.

INTRODUCTION:

We are living in an era where we are open to abundant digital imagery. We use to have blind trust on integrity and authenticity of this imagery but today's technology has depleted this trust. From the esteemed magazines to the media industry, courtrooms, fashion outlets, scientific journals, political campaigns, and the photographic jest that land in our e-mail inboxes and social media platforms. Forged photographs are appearing with a growing frequency. Without any doubt image authenticity now is a big matter of concern. There are two main categories of image forgery detection to verify the legitimacy of the manipulated image. The first one is Active method and another is Passive method for forgery detection and they are further explained in the literature. Watermarking and Steganography are two main categories under the active methods where the authentic information is inserted into the digital image. The prior stored information is used to enlighten whenever there is a need to test the authenticity of the image.

If we talk about passive techniques the most popular method to forge an image is a copy-move forgery. It is done by copying apart from the image and paste it into the same image. There are many other faster techniques like double JPEG compression, Noise Inconsistency etc.

0 After undergoing through photo-editing software, both original and manipulated image is compressed twice due to the lossy nature of the JPEG (since most images are stored in JPEG). This double compression creates specific artefacts not present in a single compression.


INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

ALTERED IMAGE

BY DANIEL VERTON

Federal intelligence agencies are studying ways to use computers and the Internet, rather than just leaflets and radio broadcasts, to shape and disseminate information designed to sway public opinion in the world's hot spots.

As part of its so-called "perception management" program, the intelligence community has for decades created misinformation to trigger political change without direct political or military involvement in countries where the United States has vested interests, such as Iraq and North Korea.

Acting on congressional recommendations to bolster research and development in information technology, intelligence agencies are turning to PCs to develop more sophisticated means of manipulating and delivering digital photos, video clips and recorded sound to portray fictitious events in hopes of provoking desirable outcomes.

Altered Egos

The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agencies plan to use similar techniques to create images and then disseminate them via the Internet in their efforts to influence events in foreign countries, such as Iraq.

Figure 1: Example of the copy-move forgery where object of two different image is copied and moved to third image. This image also tells that this forgery can very dangerous if sensitive information is altered.

LITERATURE SURVEY:

In the field of the digital forensics, the detection of the image forgery can be broadly classified into two methods. The first, method is termed as the Active method which can further be specified as digital water-making method and digital signature. These techniques are required when any alterations are done during the creation of the image. Second, the method is termed as Passive method which are having various kinds. The passive or blind forensic approaches verify the genuineness by exploring intrinsic features in the media left by acquisition devices or manipulation acts, without using any pre-embedded signals. Among all those kinds Copy-Move is one of the most general and widely used forgery detection in any image. Forgery which includes region pasting from another region of the image. This type of forgery is very common and easily done. The algorithms which can be used for such kind of forgery detection are PCA (Principle Component Analysis) and DCT (Discrete Cosine Transform). These algorithms are the most popular and one seems to be most efficient in this method. In the case of analyzing the still image, the pixel position and the pixel value is quite constant hence, the analysis of the pixels can be done easily. Based on the different forensic researches we came to know that copy-move forgery detection should be done before other detection because of its monotonous nature. In copy-move tampering changes only parts of the frame images, which is

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

similar to image copy-move, and can be detected by relatively mature image. This type of strategy can be said as a pixel comparison strategy. In this copy-move algorithm, the first work is to divide the image into adequate grey-scaled blocks. Then, these blocks are arranged into arrays and then analysis of each block is done. This same technique is when improved and made faster with constant efficiency then its extension can be used in the video forgery detection and video is divided into frames as blocks were divided into images. There are many possible challenges in the current scheme which could be irregularity of the image could lead to large computation, there might be some cases where we can see an unstable performance and since, input image could of any format, therefore, there is a possibility that algorithm couldn't stand strong in all possible permutations.

EXISTING SYSTEM:

The existing block-based forgery detection method segment the image into some overlapping blocks and obtain the tempered region by matching blocks of image pixel and transform coefficient. The existing technique needs large computation and also having large time complexity. As this system is sometimes used to solve some crucial cases and the delay in the result is unacceptable. The methods cannot address significant geometrical transform of the forged region. Hence, we can say that the existing system has high computational complexity and unstable detection performance which can be improved in the proposed system.

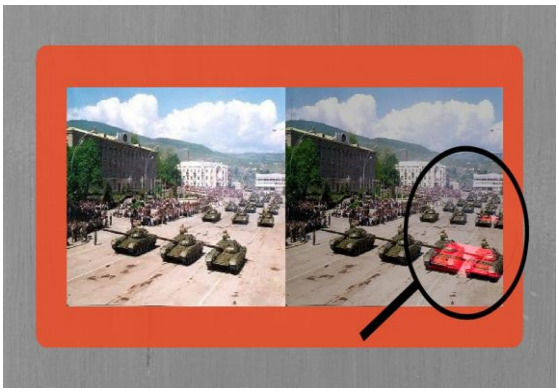

Figure 3:Example for altering sensitive information.

PROPOSED SYSTEM:

In the proposed system we are enhancing the accuracy and efficiency rate of detecting forgery in the existing system. The speed of detecting a Copy-Move forgery is also increasing in the proposed system as we eliminate the supervised data sets for matching and comparison with the forged image. In this, we use two techniques for detection of the duplicate region. The first technique is by applying PCA (Principle Component Analysis) on the small fix size image block of 32x32. The eigenvalues and eigenvector for each block are calculated. After applying lexicographic sorting, the duplicate regions of the image are automatically detected. In other proposed algorithm, matches are been searched among the DCT representation of image segments. DCT coefficients are lexicographically arranged and adjacent identical pairs are considered as potentially tampered regions to avoid the computational burden of a brute force comparison. After the lexicographical sorting, similar blocks are detected and forged region is found.
The algorithm of DCT consist of formula which is -

$$B = \sum_{k=1}^{64} \left| D(k) - Q(k) round\left(\frac{D(k)}{Q(k)}\right) \right|$$

The level of quantization is first estimated for each of 64 DCT frequencies from a region of the image which is presumed to be authentic. The inconsistencies between the DCT coefficients (D) and the estimated amount of quantization (Q) are computed as Variations in B across the image.

SYSTEM IMPLEMENTATION:

Steps for system implementation:

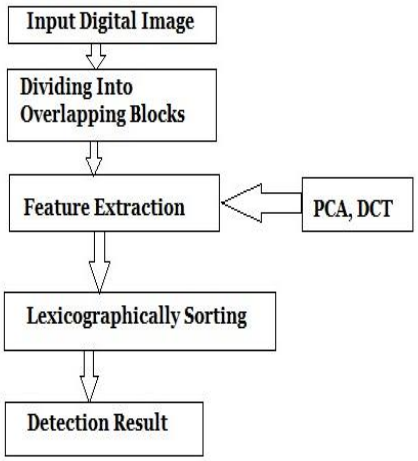

Figure 4: Block Diagram for System of Image Forgery Detection.

1. *INPUT DIGITAL IMAGE:*
The input image for our system can be taken from any local storage. For this, we can take help of UI with browse function; to import the image.

2. *DIVIDING INTO OVERLAPPING BLOCK:*
The input image is divided into the blocks which are overlapping in nature. This is done because working on the whole image in one go can be extra overhead for the algorithms which can result in lowering the accuracy and efficiency of the system. These overlapping blocks also help us to find the region of the forgery after the successful working of the algorithms because overlapping blocks tells us about the neighbouring pixels in the image.

3. *FEATURE EXTRACTION—PCA, DCT:*
PCA (Principal Component Analysis) is the common feature extraction method in image processing. PCA finds the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

eigenvectors of a covariance matrix with the highest eigenvalues and then use those to extract the data into a new sub-space of equal or fewer dimensions. It converts a matrix of n features into a new data set of less than n features that's why it reduces the number of features by constructing a new one with smaller number variable which captures a significant portion of information found in the original features. This means that a featured image can be processed similarly as an ordinary image generated by an image sensor. DCT is a powerful transform to extract proper feature for image processing. After applying DCT to the entire face image, some of the coefficients are selected to construct the feature vector. Most of the approaches in a zig-zag manner. In some cases, the low-frequency coefficients are discarded to its variation. DCT can be used to achieve a higher true feature extracting rate by using discriminate coefficients (DCS) as a feature vector. Discrimination power analysis (DPA) is based on DCT Coefficient properties and discrimination concepts. It searches the coefficient which has both powers to discriminate classes better than others. The DTA based approach achieves the performance of PCA of better with less coefficient.

4. *LEXICOGRAPHICALLY SORTING:*

In this step of lexicographical sorting, the principle components which are extracted in the previous step are sorted to arrange similar blocks close to one another. When finally, similar regions are selected based on the distance, the forged region can be detected for the PCA algorithm. Similarly, in the DCT algorithm, the calculated DCT coefficients are lexicographically arranged and the adjacent identical pairs are considered as potentially tampered region to avoid the computational burden. A refinement of this selection is based on a spatial criterion. A histogram is build based on the number of matching segments, higher the number of pair located at the same distance, higher is the probability that those pairs belong to a copy moved region.

5. *DETECTION RESULT:*

The result which we get in the end is our final resultant image which would be highlighting the regions in the image which are detected as forged and can be termed as tempered. If no forgery is detected in the image then the result would be the original image without any highlights or markings.

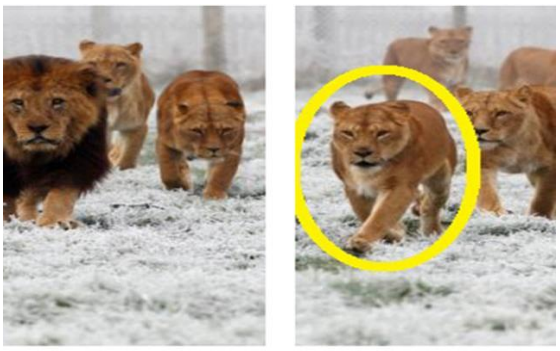

Figure 5: Example for detection of forged image.

RESULTS:

CONCLUSION:

The proposed scheme for the detection of image forgery uses feature point extraction and morphological operation. It can divide the forged region by indicating the affected pixel. The algorithm used in the proposed experiment can achieve good performance under various challenging conditions such as geometrical transform and JPEG compression. Hence the system is providing an accurate and efficient result in detecting copy-move forgery without the help of any pre-existing data set for the forged image.

FUTURE ENHANCEMENTS:

The future work may focus on increasing the accuracy rate of the proposed algorithm in images as well as in video forgery detection. Another future direction in the proposed system can be of using a variable size of overlapping blocks which are used for the morphological operations. Using the variable size of block for detection can also help in enhancing the robustness and time taken to detect the forgery. The usage of this system is generally limited to the forensics, in future this system can also be implemented to filter out the content on the social media to eliminate fake news and malicious content.

REFERENCES:

[1] Jian Li; Xiaolong Li; Bin Yang; onYear: 2015, "Segmentation-Based Image Copy-Move Forgery Detection Scheme" Xingming Sun Information Forensics and Security, IEEE Transactions.

[2] R. Sekhar and R. S. Shaji, "A methodological review on copy-move forgery detection for image forensics," Int. J. Digit. Crime Forensics, vol. 6, no. 4, pp. 34–49, 2014.

[3] Ms Kaveri S. Nehe, Ms Sneha R. Birajdar, Ms Madhuri K. Ugale, Suwarna S. Ugale, Mr Kishor N. Shedge; "Framework for Image Forgery Detection" International Research Journal of Engineering and Technology (IRJET) Volume: 06 Issue: 11.

[4] S.Saravana Kumar, R.Barath, Mrs.A.G.Jessy Nirmal, "COPY MOVE FORGERY IMAGE DETECTION" International Journal of Advanced Research in Computer Science Engineering and Information Technology Volume: 4, Issue: 3, Special Issue: 2.

[5] 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.

[6] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009, pp. 1053-1056.

[7] Ms M. H. Kore, Dr R. J. Shelke, "Techniques of Copy Move Forgery Image Detection" IJSRD - International Journal for Scientific Research & Development| Vol. 5, Issue 10.

[8] Reshma Raj, Niya Joseph, "Keypoint extraction using SURF algorithm for CMFD" Science Direct Procedia Computer science93, 6th International Conference on Advances in Computing & Communications, ICACC.