

COPY- PASTE FORGERY DETECTION USING STATISTICAL FINGERPRINTS

Amandeep Kaur¹, Harpreet Kaur²

¹Amandeep Kaur, M.Tech (CSE), Student, DIET Kharar, Punjab, India

²Harpreet Kaur, Assistant Professor, Department of CSE, DIET Kharar, Punjab, India

Abstract- A digital image is a numeric representation of a two-dimensional image. Depending on whether the image resolution is fixed, it may be of vector or raster type. Without qualifications, the term "digital image" usually refers to raster images also called bitmap images. When we see a picture on our monitor or use our digital camera (or scanner), the image we are viewing or dealing with is not continuous like a pencil drawing – it is made up of many small elements next to each other. When we have enough elements, we get the illusion of a picture or image. Early digital images (before color) appeared in black and white. The tiny elements that comprised digital images were either black or white. These two 'colors' corresponded to 1 and 0 (called BITS or BI-nary digits). Digits 1 and 0 are used in the binary (base 2) system. Thus, a map (pattern) made up of these 1's and 0's was referred to as a bit-map. All digital images are a rectangle or square. Today, the elements are called pixels.

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices. Digital image forensics aims at validating the authenticity of images by recovering information about their history. Two main problems are addressed: the identification of the imaging device that captured the image, and the detection of traces of forgeries. Forensics means the use of science and technology in the investigation and establishment of facts. So the photographs or other pictures can be transmitted to and reconverted into pictures by another computer. With the widespread availability of image editing software, digital images have been becoming easy to manipulate and edit even for non-professional users.

Keywords-Digital image Forensics, Correlation Based Measures.PSNR, RMSE.

1. INTRODUCTION

Image manipulation has become commonplace with growing easy access to powerful computing abilities. Some common image manipulation with the intension of deceiving a viewer includes:-

- Copy and paste
- Composition or Splicing

- Retouching,healing,cloning
- Content embedding or steganography

One of the most common types of image forgeries is the copy-paste forgery, wherein a region from an image is replaced with another region from the same image (with possible transformations). Because the copied part come from the same image, its important properties, such as noise, color palette and texture, will be compatible with the rest of the image and thus will be more difficult to distinguish and detect these parts. Digital image forensics is a brand new research field which aims at validating the authenticity of images by recovering information about their history. In Figure1, an example of copy-move forgery can be seen where the original image (Figure 1(a)) has one bird flying in the sky whereas in forged one (Figure (b)), Cloning tool of Photoshop has been used to show that there are two birds flying.



(a)

(b)

Figure 1. Example of Copy-Move forgery (a) original image (b) tampered image

So, Digital image forensics aims at restoring some of the lost trustworthiness of digital images.

1.2. RELATED WORK IN THE FIELD OF COPY PASTE DIGITAL IMAGE FORENSICS

Many Techniques for digital image forensics have been proposed in the literature. Some of them are discussed below.

The popular method works on block-matching procedures, which first divide the image into overlapping blocks and extract features from each block, assuming similar blocks will yield similar features. Later, a matching step takes place where the aim is to find the duplicated

blocks based on their feature vectors. A forgery detection decision is made only if similar features are detected within the same distance of features associated to connected blocks.

The DWT technique works by first applying DWT (Discrete Wavelet Transform) to the input image to yield a reduced dimensional representation. Then the compressed image is divided into overlapping blocks. These blocks are then sorted and duplicated blocks are identified using Phase Correlation as similarity criterion. Due to DWT usage, detection is first carried out on lowest level image representation. This approach drastically reduces the time needed for the detection process and increases accuracy of detection process.

The SIFT method explains if a copy-move attack has occurred and, furthermore, to recover the geometric transformation used to perform cloning. Extensive experimental results are presented to confirm that the technique is able to precisely individuate the altered area and, in addition, to estimate the geometric transformation parameters with high reliability. The method also deals with multiple cloning.

The transform-invariant features based on obtaining the features from the MPEG-7 image signature tools. Results are provided which show the efficacy of this technique in detecting copy-paste forgeries, with translation, scaling, rotation, flipping, lossy compression, noise addition and blurring. Author obtained a feature matching accuracy in excess of 90% across post processing operations, and was able to detect the cloned regions with a high true positive rate and lower false positive rate than the state of the art.

2. PROPOSED SCHEME

The goal in copy-move forgery detection is detecting duplicated image regions, even if they are slightly different from each other. A copy-move forgery is created by copying and pasting content within the same image, and potentially post processing it. As the copied part come from the same image, its important properties, such as noise, color palette and texture, will be compatible with the rest of the image and thus will be more difficult to distinguish and detect these parts. Typical motivations are either to hide an element in the image, or to emphasize particular objects.

The steps involved in proposed method are as follows:

Input: Original Image I_m , Forged Image fI_m

Output: Detected forgery region

Step1: Read the input image

Step2: Pre-process the input image, transform image into color space.

Step3: Obtain the homogeneous regions r_i for I_m and fI_m

Step4: For each r_i, r_j

Do

Step5: Compute the phase correlation using formula

Step6: Perform histogram equalization for I_m and fI_m

$$Corr(r_i) = r_i \cap r_j \quad \dots\dots\dots (1)$$

where $i \in I_m$ and $j \in fI_m$

If ($Corr (r_i) > threshold$)

Step7: Compute the feature map in detected region using formula

$$F_{map} = \frac{1}{N} \left(\sum (\det ect_{region} - \overline{\det ect_{region}}) \right) \dots\dots$$

(2)










Where N is total number of pixels

Step8: Output the detected Forgery region

2.1. EXPERIMENTAL RESULTS

The proposed algorithm is tested for the various images. In the table shown below, the first column shows the original image, the second column shows the forged image means in which the copy paste forgery is applied and the third column gives the result after applying these measurements. Here some results are given.

Table1.Result of Proposed method

Original Image	Forged Image	Output Image
		
		
		

To evaluate the performance of the proposed method, PSNR (Peak Signal to Noise Ratio) and RMSE (Root Mean Square Error) values. PSNR is widely used to measure imperceptibility between the original image and forged image. PSNR and RMSE are defined in the following equations. The similarity between the original and extract forgery image use to represent how algorithm is robust against noise that is calculated by Directional Correlation value.

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

$$RMSE = \sqrt{\frac{1}{N} \sum_{i=1}^N [y_i - \hat{y}_i]^2}$$

Following curves prove that our method gives better results than existing method. Fig 2(a) shows that the correlation coefficient values will increase. Fig 2(b) shows

that the PSNR Value will also decreased as compare with existing method. Fig 2(c) shows that the RMSE Value will also decreased as compare with existing method.

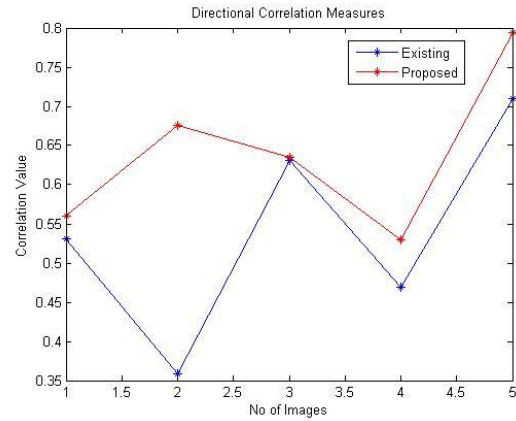


Fig 2(a) shows comparison of correlation coefficient values with the existing method.

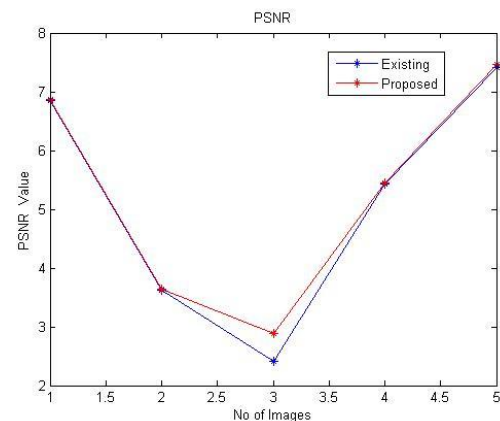


Fig 2(b) shows comparison of PSNR values with the existing method.

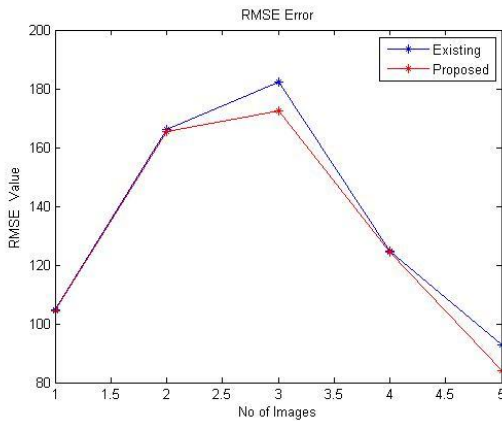


Fig 2(c) shows comparison of RMSE values with the existing method.

3.CONCLUSION

The proposed method gives the better result than the existing. By applying these measurements the error rate will be minimized and the forgery detection rate will be increased. By using these measurements the forgery region will be better highlighted as compared to previous results. In the previous results the forgery part detected by using the boundary box but using this measurements the forgery part is better highlighted from the image which will be easily identified by the user.

REFERENCES

- [1] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Transactions on Signal Processing*, vol. 53(2), pp. 758–767, 2005.
- [2] M.C. Stamm, "Forensics Detection of Image Manipulation Using Statistical Intrinsic Fingerprints", *IEEE Transactions on Information Forensics and Security*, vol. 5 No 3, 2010
- [3] M.K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," *Proc. ACM Multimedia and Security Workshop*, New York, pp. 1–9, 2005.
- [4] M.Wu A. Swaminathan and K. J. Ray Liu, "Image tampering identification using blind deconvolution," *Proc. IEEE ICIP*, 2006.
- [5] P.Kakar and N.Sudha "Exposing Post processed Copy-Paste Forgeries through Transform-Invariant Features", vol. 206, no. 1-3, pp. 178–184, 2011.
- [6] S.Bayram, H.T.Sencar and N.Menon "A Survey of Copy-Move Forgery Detection Techniques", submitted to ICASSP 2009, 2009.
- [7] S.Khan and A.Kulkarni, "Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform" *International Journal of Computer Applications* (0975 – 8887) Volume 6– No.7, September 2010.