

Elucidating Digital deception: Spot counterfeit fragment

Neeraj Mishra*, Asmita Haveliya**

*Asst. Prof., Department of Electronics and Communication Engineering
R D Foundation Group of Institution, Ghaziabad, India.

**Department of Electronics and Communication Engineering
ASET, Amity University, Lucknow, India

Abstract

An ordinary person always has confidence in the integrity of visual imagery and believes it without any doubt. But today's digital technology has eroded this trust. A relatively new method called image forgery is extensively being used everywhere. This paper proposes a method to depict forged regions in the digital image. The results for the proposed work are obtained using the MATLAB version 7.10.0.499(R2010a). The projected design is such that it extracts the regions that are forged. The proposed scheme is composed for uncompressed still images. Experimental outcome reveals well the validity of the proposed approach.

Keywords: digital forgery, image processing, image falsification

I. INTRODUCTION

Image forgery, an immensely popular and tremendously simple technology due to various computer graphics editing software such as adobe Photoshop, GIM and Corel paint shop is evolving at breakneck speed. Fake images are created to generate deception in users mind. The manipulation of images through forgery influences the perception an observer has of the depicted scene, potentially causing the intended after effects. By using open source framework of manipulating the images, it is never stopping in its astonishing capabilities. It seems like the concept is of modern scenario of tech boom but image forgery's concept can be traced back as early as the beginning of 19th century. A person named hippoyo bagaed tried to create a fake image of him committing suicide. In modern digitized world a digital image is simply a grid of numbers and it is conceivable for an artist to create a computer generated image by painting a grid of numbers and represent any object or scene that could be captured with digital camera. In other words in digital image forgery we change the material elements of a document and represent the changes as true copies of a real one.

Image forgery, in its absolute form can broadly be classified into 3 groups;

1. IMAGE RETOUCHING,
2. IMAGE SPLICING,
3. COPY - MOVE ATTACK.

Image retouching is a very mild type of image forgery which does not significantly changes the image, but it enhances or reduces the intensity and certain features of the image.

In magazine photographs it is used to enhance the visual effects.

Image retouching is a type of digital image forgery, in which 2 or more images are combined to create a fake and dramatized image. Simple image graphic frameworks can be utilized to learn image retouching with little expertise.

Copy move attack uses a portion of the original base image as its source and then moves it to a point in the same source. Parts of the original image is copied, moved to a desired location and pasted. The motive may be to conceal specific details or to duplicate certain features of the digital image.

To eliminate the irregularities between the original and pasted region, blurring is used.

With the evolvement of image forgery techniques, it is now virtually impossible to isolate the fake images from the real one. Several detection techniques have been developed to check and detect image forgery. This branch is called digital image forensics. The projected approach is been verified for PNG, JPEG, TIF and still GIF file formats. Proposed work on the whole, detects areas where an image has been manipulated. An example of a digital forgery is shown in Figure 1. The figure 1(b) shows, Image of the mountain with a missing lady on rocks. Image of the lady from the rocks was sliced from the original image, fig 1(a). Figure 1 is a well example of probable looking forgery. The file format of the images in figure 1 is taken with JPEG extension.





Figure 1 Example of a digital forgery with JPEG extension.1 (a) original image.1 (b) forged image. Another example of a digital forgery is shown in Figure 2. As the figure 2(b) shows, two different images, Image of the dog and a scenery are merged together to give the concluding image. Image of dog was sliced from some different image and pasted on the image of the scenery. Figure 2 is although an example of improbable looking forgery, but capable to through light on the subject of forgery. The file format of the images in figure 2 is taken with PNG extension.



Figure 2 Example of a digital forgery with PNG extension.2 (a) original image.2 (b) sham image. Another example of the false digital image sham is shown in Figure 3. As the figure 3(b) shows, two different images, Image of the landscape and a sun with great shine are fused together to give the ultimate image. Image of sun was segmented from some different image and pasted on the image of the landscape. The file format of the images in figure 3 is taken with TIF extension.



Figure 3 Example of a digital forgery with TIF extension.3 (a) original image.3 (b) phony image. The next figure, fig 4 is a still GIF format image, fig4 (b) is the forged image. From original image a car is been sliced to formulate it appear like a phony image.



Figure 4 Example of a digital forgery with GIF extension.4 (a) original image.4 (b) bogus image.

II. LITERATURE SURVEY

Image forgery, an immensely popular and tremendously simple technology due to various computer graphics editing software such as Adobe Photoshop, GIMP and Corel Paint Shop is evolving at breakneck speed. Fake images are created to generate deception in users' minds. There are a lot of image forgery techniques available for forging digital data. As described by S. Khan, blind image forensics gives a nice way of detecting the copy-move forgery [1]. As the technology today is full of powerful image processing tools, therefore, the manipulation of digital images is quite easy. Sir Ghorbani, M presented an improved algorithm based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform Quantization Coefficients Decomposition (DCT-QCD) to detect the cloning forgery in his paper titled "DWT-DCT (QCD) based copy-move image forgery detection" [2]. In retouch type of image forgery, blurring image is the most commonly used technique. By using blur estimation and abnormal hue, Fei Ping proposed in his paper "Digital Image Forgery Forensics by Using Blur Estimation and Abnormal Hue Detection", a digital image forgery forensics scheme [3]. Sir Zhen Zang in one of his papers, associating with the common forge methods, proposed the

process of passive-blue detection of digital image forging method. He also reviewed the latest development of the passive-blind detection of image forging method; mainly including the detection of copy-move forgery, detection of blur forgery and detection of re-sample forgery [4]. A new algorithm to detect digital image forgery based on cellular automata and data embedding in spatial domain was presented in year 2011 by respected A.P. Tafti in a paper titled "Digital image forgery detection through data embedding in spatial domain and cellular automata" [5]. He used region-based specification method on the input image to specify the desired regions of interest. As already described, there is a variety of software available in the market for image forgery; therefore, it has become a serious social problem. Junwen Wang proposed an efficient and robust algorithm for detection of a specific category of digital image forgery known as region duplication forgery, which is done by copying a block of an image and pasting it on to some other block of the same image [6]. He also proved the efficiency of this method over other existing methods. He presented this approach in his paper titled "Detection of Image Region Duplication Forgery Using Model with Circle Block". It may be interesting to know that image manipulations of different types may be visible in a suitably designed log-likelihood image. This theory is presented by J. Grim in one of his works. In his work, he explained how to transform the original image by using the estimated mixture. This estimated mixture is a local Gaussian mixture which is presented as an application of local statistical models [7]. Another useful technique of image forgery is passive-blind color image forgery detection, which is proposed by Sutthiwan, P. It is a combination of image features extracted from image luminance by applying a rake-transform and from image chrominance by using edge statistics. He promised to overcome with the challenges in the field of image forgery [8]. Due to advancement and growing popularity of image editing software, images are manipulated easily. This not even leaves a single visible clue that could help to identify the difference between original image and forged image. The presence of anti-elements in the society leads to wrong and abusive use of this technique. Hence, there is a strong need felt to find effective as well as fast ways to detect forgeries in the image. Image copy-move forgery detection method based on SURF (Speed Up Robust Features) as presented by Xu Bo can be visualized as a robust technique [9]. As can be seen clearly that in this paper copy-move technique of image forgery is discussed. Reason for doing so is the belief of the authors that it is the most efficient method for detection of forged images. Sir Zhao Junhong presented a new approach based on one improved LLE [10]. This new approach can detect not only copy-move areas but also the fused edges as claimed

by him. Sir Li Kang has also done work in this field. He said that the goal in detection of copy-move forgeries is to detect image areas that are same or extremely similar. He investigated the problem of detecting the copy-move forgery and described an efficient and reliable passive-blind detection method [11]. However, Dongmei Hou proposed a new image division method to detect image copy-move forgery. He has achieved this by crossing shadow technique [12]. The work of different authors in this particular area of image forgery (detection of copy move forgery) is remarkable. Sir Hailing Huang explained a new method that works by first extracting SIFT descriptors of an image, which are invariant to changes in illumination, rotation, scaling etc [13]. Owing to the similarity between pasted region and copied region, descriptors are then matched between each other to seek for any possible forgery in images. Experiments have proved the efficiency of this system to a great extent. A way of fighting to the problem of forgery is copy-move forgery detection based on SVD in digital image as demonstrated by Zhang Tang [14]. This method has also produced the desired results easily. Sir Bayram proposed to use the notion of counting bloom filters as an alternative to lexicographic sorting, which is a common component of most of the proposed copy-move forgery detection schemes and this approach can be considered as another step towards detection world [15].

III. PROPOSED WORK

The tactic followed in this proposed effort can be applied by giving a picture of the misplaced or omitted or new piece in the sham image then tagging and deleting the allied components and thus detecting the forged region in the image, followed by marking the detected section black, to show us the bogus section.

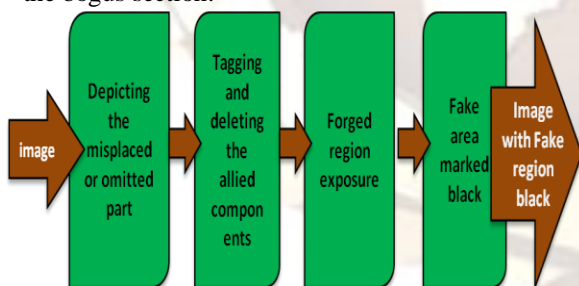


Figure 5 Block diagram of the methodology approached.

The methodology followed in the proposed work is explained using the block diagram in figure 5 followed by figure 6.

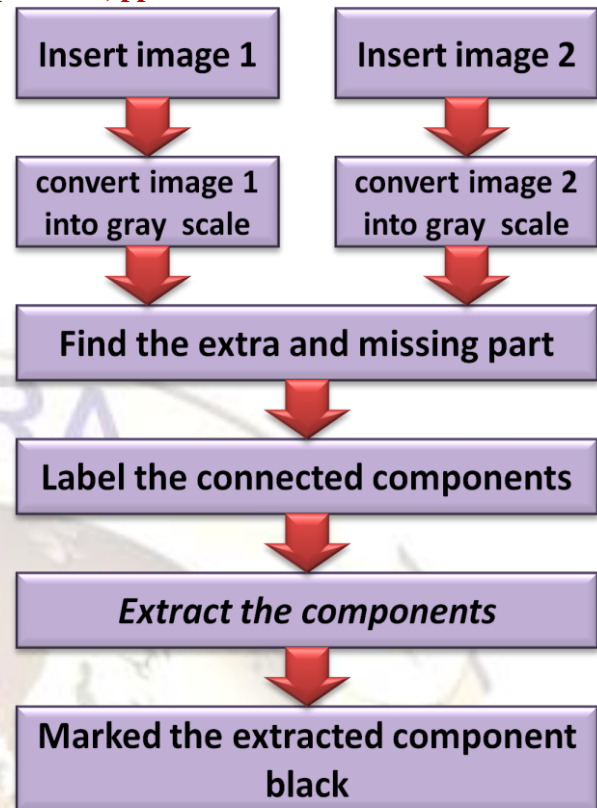


Figure 6 system organizations.

IV. RESULTS

We have presented an efficient and robust technique that automatically detects duplicated regions in an image. Here a replica-attach tampering is adopted to evaluate the capability of forgery detection. The block mismatching in the original and sham image generates a black square. In this paper, a passive scheme to achieve forgery detection is developed for uncompressed images. The next figures 7, 8, 9, 10 represent the result obtained for the images in figure 1, 2, 3, and 4 respectively.

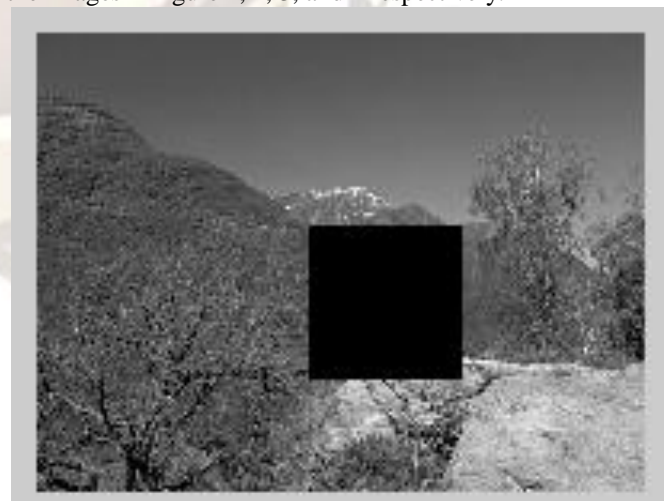


Figure 7 exposure of sham region for figure 1 using a black patch.



Figure 8 exposure of sham region for figure 2 using a black patch.



Figure 9 coverage of fraud region for figure 3 employing a black patch.




Figure 10 disclosure of sham section for figure 4 using a black patch.

CONCLUSION

The very unproblematic accessibility of inexpensive and prevailing image processing and editing software, makes image manipulation relatively easy, for exploitation or for enjoyment, and even a person with lukewarm skills can introduce alteration in images to a drastic frontier. The results for the proposed work are obtained using the MATLAB version 7.10.0.499(R2010a). The projected design is such that it extracts the component that has large size and will avoid small and negligible components. The proposed scheme is composed for uncompressed still images. Experimental outcome reveals well the validity of the proposed approach.

REFERENCES

- [1] Khan, s., "Robust method for detection of copy-move forgery in digital images", *Signal and Image Processing (ICSIP), 2010 International Conference on* 15-17 Dec. 2010, 69-73
- [2] Ghorbani, M., "DWT-DCT (QCD) based copy-move image forgery detection", *DWT-DCT (QCD) based copy-move image forgery detection*, 1-4
- [3] Fei ping, "Digital Image Forgery Forensics by Using Blur Estimation and Abnormal Hue Detection", *Photonics and Optoelectronic (SOPO), 2010 Symposium on* 19-21 June 2010, 1-4
- [4] Zhen Zang, "A survey on passive-blind image forgery by doctor method detection", *Machine Learning and Cybernetics, 2008 International Conference on* 12-15 July 2008, 3462-3467
- [5] Tafti, A.P., "Digital image forgery detection through data embedding in spatial domain and cellular automata", *Digital Content, Multimedia Technology and its Applications (IDCTA), 2011 7th International Conference on* 16-18 Aug. 2011, 11-15
- [6] Junwen Wang, "Detection of Image Region Duplication Forgery Using Model with Circle Block", *Multimedia Information Networking and Security, 2009. MINES '09. International Conference on* 18-20 Nov. 2009, vol-1, 25-27
- [7] Grim, J., "Digital Image Forgery Detection by Local Statistical Models", *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on* 15-17 Oct. 2010, 579-582
- [8] Sutthiwan, P., "Rake transform and edge statistics for image forgery detection", *Multimedia and Expo (ICME), 2010 IEEE International Conference on* 19-23 July 2010, 1463-1468

- 
- The background of the page features a large, faint watermark of the IJERA logo. The logo consists of a circular emblem with a globe in the center, surrounded by a laurel wreath. The acronym 'IJERA' is written in a stylized font across the top of the emblem.
- [9] Xu Bo, “Image Copy-Move Forgery Detection Based on SURF”, *Multimedia Information Networking and Security (MINES), 2010 International Conference on* 4-6 Nov. 2010, 889-892
- [10] Zhao Junhong, “Detection of Copy-Move Forgery based on one improved LLE method”, *Advanced Computer Control (ICACC), 2010 2nd International Conference on* 27-29 March 2010, 547-550
- [11] Li Kang, “Copy-move forgery detection in digital image”, *Image and Signal Processing (CISP), 2010 3rd International Congress on* 16-18 Oct. 2010, vol-5, 2419-2421
- [12] Dongmei Hou, “Image copy-move forgery detection based on “crossing shadow” division”, *Electric Information and Control Engineering (ICEICE), 2011 International Conference on* 15-17 April 2011, 1416-1419
- [13] Hailing Huang, “Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm”, *Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on* 19-20 Dec. 2008, vol-2, 272-276
- [14] Zhang Tang, “Copy-Move Forgery Detection Based on SVD in Digital Image”, *Image and Signal Processing, 2009. CISP '09. 2nd International Congress on* 17-19 Oct. 2009, 1-5
- [15] Bayram, S., “An efficient and robust method for detecting copy-move forgery”, *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on* 19-24 April 2009, 1053-1056.