Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Optimization of Copy-Move Forgery Detection Technique

Amanpreet Kaur
Department of Computer Science and Engineering, Lovely Professional University, Punjab, India.

Richa Sharma
Department of Computer Science and Engineering, Lovely Professional University, Punjab, India.

Abstract: Digital images are foremost source for information transfer. Due to advancement of the technology, images are now not treated as reliable source of information. Digital images can be edited according to the need. Adding and deleting content from an image is most easiest and popular way of creating image forgery, which is known as copy-move forgery. Digital Image Forensics is the field that deals with the authenticity of the images. Digital image forensics checks the integrity of the images by detecting various forgeries. In order to hide the traces of copy-move forgery there are editing operations like rotation, scaling, JPEG compression, Gaussian noise called as attacks, which are performed on the copied part of the image before pasting. Till now these attacks are not detected by the single method. The novel approach is proposed to detect image forgery by copy-move under above attacks by combining block-based and keypoint-based method.

Keywords: Digital image forensics, copy-move forgery, passive blind approach, keypoint-based and block-based methods.

I. Introduction

Digital images are the major source of information in today's digital world. Due to their ease of acquisition and storage they are the fastest means of information transfer. Images can be used as an evidence for any event in the court of law. The images broadcasted in any TV news are accepted as the certificate for the truthfulness of that news. Digital images are being used in many applications ranging from military to medical diagnosis and from art piece to user photography. Hence the digital image forensics emerges as fast growing need of the society. Thus the images are required to be authentic. Due to technology advancement and availability of low-cost hardware and software tools it is very easy to manipulate the digital images without leaving the visible traces of manipulation. It has become difficult to trace these operations. As consequences, the integrity and authenticity of digital images is lost. This modification of images can be used for some malicious purpose like to hide some important traces from an image. Thus using modified

images to convey wrong information. In order to identify the integrity of the images we need to detect any modification on the image. Digital Image Forensic is that branch of science that deals at exposing the malicious image manipulation. Figure 1 is showing a sample case of image forgery.

Figure 1: Example of copy-move forgery. Left: The original image. Right: The tampered image.

A. Forgery Detection

Digital image forensics is branch that deals with the authenticity of the images. It has two principal approaches to detect forgery, first active approach which includes watermarking and steganography. These are implemented at the time of image acquisition. Active approaches require a special hardware implementation to mark the authentication of the digital image, like embedding the digital signature in the image or coding the image into some other form. The watermarking consists of hiding a mark or a message in a picture in order to protect its copyright at the time of image acquisition and to check the authenticity this message is extracted from the image and verified with the original watermarks. If image is not manipulated these watermarks will remain same else they will not match the original watermarks. Hence this method relies on the source information before hand. Some camera sources do not embed watermarks into image therefore this method is not that useful.

Second, passive approach which do not require any prior information about the image and depends on traces left on the image by different processing steps during image manipulation. Passive approach also determines the amount and the location of forgery in the image. There are two methods of passive approach. First, image source identification, it identifies the device used for the acquisition of the digital image. It tells that the image is computer generated or digital camera image. In this method the location of forgery in image cannot be determined. Second, tampering detection, it detects the intentional manipulation of images for malicious purposes. Image manipulation is denoted as tempering when it aims at modifying the content of the visual message. There are various techniques to manipulate digital image by copy-move image, image composition and tampering image features. In copy-move forgery the single image is used to perform forgery within that image. In image composition two or more images are combined together to form another image. In tampering image features the characteristics of the images like brightness, contrast is manipulated to change the image meaning.

B. Copy-Move Forgery

Copy-Move image forgery is the widely used technique to edit the digital image. In this technique a part of the image is copied and pasted to another part of the same image. Copy-move simply requires the pasting of image blocks in same image and hiding important information or object from the image. Thus this changes the originality of the image and put at stake the authenticity of that image. As the copied blocks are from same image they have same properties as the other blocks of same image hence this makes it very difficult to detect forgery by humans. A copy-move forgery introduces a correlation between the original image area and the pasted content. It is often necessary to resize or rotate portions of an image to create a convincing forgery. Good forgery detection method should be robust to manipulations, such as scaling, rotations, JPEG compression and Gaussian Noise addition made on the copied content.

II. Related Work

In robust match algorithm, Fridrich and Lucas [2] used Discrete Cosine Transform (DCT) for the detection. It begins from upper left corner to the lower right corner while sliding a B×B block. For each block, the DCT transform is calculated and quantized. Then coefficients are matched with each other. However this method fails for any type of geometrical transformations of the query block e.g. rotation, scaling etc.

A.C. Popescu *et al.* [3] proposed a Principal Component Analysis (PCA) on image to give a reduced dimension representation. In this firstly the PCA is applied to fixed size image blocks to reduce dimensions and then lexicographic sorting is performed. This is robust to small variations in the image due to additive noise or lossy compression.

Luo *et al.* [4] applied color information for blocks. The whole block is divided into four sub blocks and one considers average of red, blue and green color values. Results show this method to be robust to attacks like, JPEG compression, Gaussian blurring and additive noise.

Kumar Vivek *et al.* [5], proposed an approach that divides blocks in sub blocks and feature values are calculated. It is good to detect copy move forgery JPEG compression, rotation (up to some limit), Gaussian Noise and smoothing. This method is not robust to detect attacks like of rotation by an arbitrary degree and for scaling.

B.L. Shivakumar *et al.* [6], In this method Harris Interest Point detector, to detect the corners is used along with SIFT descriptors to detect copy - move forgery and then KD-Tree is used for matching the features. This method was not robust to rotation and noise.

V. Christlien *et al.* [7], In this paper the analysis of different algorithms is done to evaluate their performance. As a result it was shown that different keypoint-based methods like SIFT and SURF, and block-based methods like DCT, PCA, KPCA, DWT, perform well and they can be combined as to get better result.

III. Proposed Methodology

Various techniques have been proposed, like DCT, PCA, KPCA, SIFT, SURF, to detect copy-move forgery. An efficient copy-move technique should be robust to attacks like losses due to compression, addition of noise, rotation and scaling. Therefore in this method the aim is to detect the forgery even after all the above attacks are made on copied content of the image in order to hide the traces of forgery. It is proposed to combine the two techniques to get optimised result.

V. Christlien *et al.* [7], analysed that keypoint-based methods like SIFT and SURF are best to detect image forgery under scaling and rotation attacks, and block-based methods like DCT, PCA and KPCA are best to detect forgery under Gaussian noise and JPEG compression attacks. So to detect image forgery under rotation, scaling, JPEG compression and Gaussian noise, keypoint-based method and block-based method can be combined.

The steps followed to detect tempering are, first detect the image features by using key-point based method and block-based method feature extraction. These features are then matched with the each other to find similar features within same image. Detected pixels with corresponding matching features are highlighted to show the forgery location.

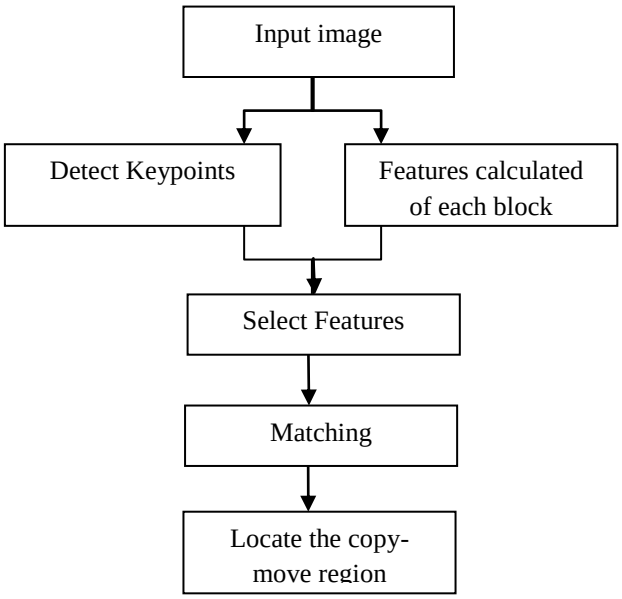

Figure 2: Configuration of Copy-Move Digital Image Forgery Detection Method.

IV. Conclusion

Digital images can be easily edited by using copy-move forgery. It was observed that keypoint-based method like SIFT and SURF are best to detect image forgery under scaling and rotation attacks, and block-based methods like DCT, PCA and KPCA are best to detect forgery under Gaussian noise and JPEG compression attacks, combining these methods we can detect forgery under above attacks by single method. In this way optimization of copy-move forgery detection technique is achieved by increase in number of attacks detected with single method. In future work the different methods can be combined to detect more number of attacks than abovementioned.

References

[1] Redi Judith, Taktak Wiem, Dugelay Jean-Luc, "Digital image forensics: a booklet for beginners," *Multimedia Tools and Applications*, vol. 51, no. 1, pp. 133-162.

[2] J.Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in digital Images," *Proceedings of Digital Forensic Research Workshop*, 2003.

[3] A.C. Popescu and H. Farid , "Exposing digital forgeries by detecting duplicated image regions," *Technical Report TR2004-515*, Dartmouth College, 2004.

[4] W .Luo, J. Huang, and G. Qiu, "Robust Detection of Region Duplication Forgery in Digital Image," *in Proceedings of the 18th International Conference on Pattern Recognition*, vol. 4, pp. 746-749, 2006.

[5] Kumar Vivek and Tripathi R.C., "Fast and Efficient Region Duplication Detection in Digital Images Using Sub-Blocking Method," *in International Journal of Advanced Science and Technology*, vol. 35, pp. 93-102, 2011.

[6] B.L.Shivakumar, Dr. S.Santhosh Baboo, "Automated Forensic Method for Copy-Move Forgery Detection based on Harris Interest Points and SIFT Descriptors," *International Journal of Computer Applications*, vol. 27, no. 3, 2011.

[7] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches", *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, 2012.

