Copy-Move Forgery Detection using DCT and SIFT

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 the most prevalent way to spread a message. So the authenticity of images is very essential. But due to advancement of the technology the editing of images has become very effortless. Copy-move forgery is most basic technique to alter an image. In this one part of image is copied, called as snippet, and pasted within same image and most likely post-processing it. Considerable number of algorithms is proposed to detect different post-processing on snippet of image. In this paper novel approach is proposed to detect combination of different post-processing operations by single method. It is analyzed that block-based features method DCT is robust to Gaussian noise and JPEG compression, secondly the keypoint-based feature method SIFT is robust to rotation and scaling. Thus by combining SIFT and DCT we are able to detect forgery under post-processing operations of rotation, scaling, Gaussian noise, and JPEG compression and thus the efficiency to detect forgery improves.

General Terms
Digital Image Forensics.

Keywords
Digital image forensics, copy-move forgery, keypoint-based and block-based methods, SIFT and DCT.

1. INTRODUCTION
Digital images are the foremost source of information in today's digital world. Due to their ease of acquisition and storage they are the fastest means of information convey. 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.

In today's scenario due to advancement of computers and availability of low-cost hardware and software tools it is very effortless to manipulate the digital images without leaving the visible traces of manipulation. It has become difficult to trace these manipulations. 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 modified images are used to transmit incorrect information. In order to identify the integrity of the images we need to identify any modification on the image. Digital Image Forensic is that branch of science that deals at exposing the malicious image manipulation. In figure 1 sample case of image forgery is depicted.

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

1.1 Approaches to Detect Forgery
Digital image forensics 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 tampering when it aims at modifying the content of the visual message. There are various techniques to manipulate digital image by copy-move forgery, 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.

1.2 Copy-Move Forgery

Copy-Move image forgery is the widely used technique to edit the digital 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 puts at stake the authenticity of that image. As the copied blocks are from same image they have same properties as the other blocks of image hence this makes it very difficult to detect forgery. The copied content of image which is used to perform forgery is called snippet. A copy-move forgery introduces a correlation among the original image area and the pasted content. It is often necessary to perform post-processing of snippet of the image before pasting to create a convincing forgery. Good forgery detection method should be robust to post-processing operations, such as scaling, rotations, JPEG compression and Gaussian Noise addition. There are considerable numbers of algorithms available focusing on different post-processing on snippet.

In this paper it is proposed to detect combination of different post-processing operations by single method. Our method is combination of block-based and keypoint-based feature extraction technique. By this method we are able to detect those forgeries which may be missed by single technique.

2. RELATED WORK

In robust match algorithm, Fridrich and Lucas [2] used DCT (Discrete Cosine Transform) for the detection. It was based on quantized DCT coefficient of each overlapping block of the image. However this method fails for any type of geometrical transformations of the query block e.g. rotation, scaling.

As in robust method the number of features extracted are enormous, Popescu *et al*. [3] proposed a Principal Component Analysis (PCA) on image to give a reduced dimension representation. In this PCA is applied to fixed size image blocks to reduce dimensions and then matching the features extracted. This method is robust to small variations in the image due to additive noise or lossy compression, thus the accuracy to detect forgery was compromised at rate. In Li. *et al*. [5] a method of features representation by Singular Value Decomposition on coefficients of Discrete Wavelet Transform blocks. These methods were block based methods as they are applying features extraction technique on each overlapping block of image. A keypoint based methods were proposed to overcome the rate complexity of block based method. Amerini *et al.* [7], proposed the method of detection using scale invariant feature transform (SIFT) keypoint. It detects the keypoint and match them using nearest neighbour search. This method is robust to rotation and scaling but cannot detect forgery by smooth surfaces.

In the paper, V. Christlien *et al.* [8] analyzed different algorithms based on 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 under some post-processing operations. It was concluded that if we combine these methods we cloud get better results.

3. METHOD

The proposed approach is based on distinct set of two features. These features are extracted by two different approaches, block-based and keypoint-based. The block-based method DCT and keypoint-based method SIFT is applied to extract features set. The set of features extracted using DCT (Discrete Cosine Transforms) are invariant to JPEG compression and Gaussian noise addition, due to strong energy compaction property of DCT coefficients. The detection method of DCT [2] consists of following steps:

1. The square block of size 16×16 pixels is slid over entire image starting from upper left corner to lower right corner. For each block the DCT is calculated and then quantized. The resultant block is stored as one row in the matrix A. The matrix will then have (M-b+1)(N-b+1)/4 rows and 15 columns in proposed algorithm, because for computational speedup the blocks at step of 2 are evaluated and for each block only high energy values(15 values) are stored as column and (x, y) location of the block in image is stored in different matrix.
2. The rows of the matrix A are then lexicographically sorted so that the identical rows are moved together.
3. For each identical rows (x_1,y_1) and (x_2,y_2) the shift vector is computed as:
$$s = (s_1, s_2) = (x_1-x_2, y_1-y_2).$$
normalise s so that shift vector –s and s corresponds to same shift vector, and for each shift vector a counter C is incremented as many times as the same shift vector is computed:
$$C(s_1,s_2) = C(s_1,s_2) + 1.$$
4. The shift vector counter greater than some threshold T, is examined and the corresponding matching blocks which contribute to that shift vector are highlighted to mark copy-move forgery. The threshold T, used in our experiment is set to maximum of the shift vector counter.

The results of proposed algorithm show that even after the blocks are evaluated at a step of 2 pixels the efficiency of the algorithm is maintained and the computational time is decreased as compared to conventional lexicographical sorting.

The second feature set is of SIFT (Scale Invariant Feature Transform) keypoints. The keypoints extracted by SIFT are invariant to rotation and scaling because orientation are assigned to each keypoint detected. The basic step is to extract local interest points as keypoints and assign local descriptor to each keypoint. The descriptors so formed are unique fingerprint of keypoints and thus they are matched with each other using best bin first algorithm based on their Euclidean distance. The method of SIFT [6] is as follow:

1. Scale-space extrema detection: SIFT features are extracted on different scale-space representation of the input image. The levels of scale-space are obtained by Gaussian blur, in vertical level, and sub-sampling, in horizontal levels, of the image resolution at next level.

$$L(x,y,\sigma) = G(x,y,\sigma) \times I(x,y).$$

Where L is the convolution of original image I on (x,y) location by Gaussian Blur operator G at scale σ for blur.

Two consecutive images in a same vertical level are subtracted to get Difference of Gaussian (DoG) given as:

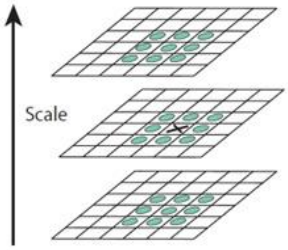
$$D(x,y,\sigma) = (G(x,y,k\sigma) - G(x,y,\sigma)) \times I(x,y)$$
$$= L(x,y,k\sigma) - L(x,y,\sigma).$$

2. Keypoint localization: In this step the maxima/minima is located within the three consecutive DoG images obtained in first step.

Figure 2: Locate maxima/minima in vertical level [6].

X is marked as keypoint if it is greatest or least among all neighbouring pixels in current scale, the scale above and the scale below. A lot of keypoint are generated so the keypoints on edge and low contrast keypoints are eliminated to get only particular keypoints..

3. Orientation assignment: The gradient direction and magnitude is calculated around each keypoint and the



prominent orientation (direction) is assigned to that region. This orientation is rotation invariance. The gradient magnitude m(x,y) and orientation θ(x,y) are calculated as:

$$m(x,y) = ((L(x+1,y) - L(x-1,y))^2 + (L(x,y+1) - L(x,y-1))^2)^{1/2}$$
$$\theta(x,y) = \tan^{-1}((L(x,y+1) - L(x,y-1)) / (L(x+1,y) - L(x-1,y))).$$

4. Keypoint descriptor: Now keypoints are detected and orientations are assigned, SIFT descriptors are unique fingerprint for that keypoint. Descriptors consist of histogram of 128 elements, obtained from 16×16 pixel area around corresponding keypoint which is further divided into sixteen 4×4 windows. For each 4×4 window, gradient magnitude and orientation are calculated and added into histogram of 8 bins. So for all sixteen 4×4 regions we will have orientation in 8 bins thus 4×4×8 = 128 numbers which are normalized to get feature vector for the respective keypoint.

At the end will we have N keypoints for the image I, described by f = {x, y, scale, orientation}, and descriptor d = f×128. These descriptors are used further for matching the keypoints. The best match is found by best bin first algorithm based on minimum Euclidean distance for invariant descriptor vector. An image is passed to both the methods and output of these methods is shown on the image. Thus if one method fails to detect the forgery it is detected by the second method and chances to detect forgery are increased.

4. RESULTS

The method was applied to the images from the database of [7] and [8]. It contains 100 original images and various types of post-processed copy-move forgery were applied to snippet of those images. Proposed algorithm method was able to detect the forgeries. In figure 3, are the few images with copy-move forgery and the output detection of forgeries by proposed algorithm. Red patches are by DCT and yellow lines are by SIFT on the output image by the proposed algorithm. Results have shown that proposed work can detect copy-move forgery when the post-processing operations like rotation, scaling, JPEG compression, Gaussian noise are applied to snippet before pasting and also when the smooth regions are used to perform content hiding. The table 1, shows the comparative analysis with DCT and SIFT of the proposed algorithm. Proposed algorithm works under all the forgery mentioned whereas other methods DCT and SIFT does not give results under few forgeries.

Table 1: Comparative analysis of results

Methods	**Copy-Move Forgery by:**				
	Rotating Snippet	Scaling Snippet	JPEG Compression on Image	Adding Gaussian Noise to Snippet	Snippet of Smooth Region
DCT	No	No	Yes	Yes	Yes
SIFT	Yes	Yes	No	No	No
Proposed Algorithm	Yes	Yes	Yes	Yes	Yes

Figure 3: Above images are tampered and below are the results of forgery detection by proposed algorithm.

There may be false detection like one or two red patches or single yellow line. Such false detection is not forgery because they are not present in cluster. The forgery is said to be detected if output image contains cluster of red patches or yellow line, marking the copy-paste of that area.

Also, as we can see from figure 4(a) and 4(b), that SIFT method is not efficient to detect forgery by smooth surfaces (grass, sky, etc), in such cases the DCT is more efficient. In images where forgery is by multiple copies or scaling is performed on snippet, figure 4(c), then DCT is not an efficient method, in such cases the SIFT is used to detect forgery.

5. CONCLUSION

In order to perform non-distinguishable copy-move forgery post-processing of snippet is performed. Proposed algorithm can detect forgery under post-processing operations like rotation, scaling, compression and noise. Results have shown that if one technique in method fails to detect forgery the other technique detects it and vice-versa and hence the detection rate is increased. It is also shown that the proposed block-based method requires less time than the conventional block-based method and efficiency is maintained. The computational time required by block-based method is more than the keypoint-based method due to the number of feature vector involved which is an important criterion to detect the forgery, so the efficiency achieved to detect forgery need to be high even at the cost of time due to legal factors involved.

In future work the method can be extended to detect forgery by more post-processing operations on snippet.

(a) **(b)** **(c)**

Figure 4: The above images are forged and below are the output detected by one technique in proposed algorithm. (a) and (b) Tampering detected by DCT where patches of grass was used perform forgery. (c) Tampering detected by SIFT as the copied part was scaled and multiple copies were pasted, DCT partially detected the forgery.

6. ACKNOWLEDGMENT

I would like to thank my mentor, Richa Sharma and department of Computer Science and Engineering of Lovely Professional University, for guidance and many helpful suggestions throughout the course of research work. Special thanks to Mr. Sonit Singh, all my friends and family, without whose support this work would not have been possible.

7. 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, 2011.

[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] G. Li, Q. Wu, D. Tu, and S. J. Sun, "A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," *in Proceedings of IEEE ICME*, Beijing, China, 2007.

[6] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, vol. 2, no. 60, pp. 91-110, 2004.

[7] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based Forensic Method for Copy-Move Attack Detection and Transformation Recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, 2011.

[8] 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, pp. 1841-1854, 2012.