A Fast and Robust Approach to Detect Copy-Move Forgery in Digital Images

Manish Deoli
Department of Information Technology
HNBGU, Srinagar (Garhwal)
Uttarakhand, India

Jyoti Joshi
Tadpole Store, Okhla Phase-I
New Delhi, India

ABSTRACT
In the present world, digital images and videos are our main source of information and these can be easily manipulated to conceal some meaningful information by using largely available powerful and sophisticated image editing tools. So in this era of illusions, verifying the authenticity of images and locating the tampering regions without using any prior knowledge is an important area of research. Copy-move forgery is one of the mostly used forgery technique. Many block matching algorithms are suggested to deal with this type of forgery but still there are some issues which are not properly addressed and need more attention such as time complexity. With increasing image size the execution time of detection algorithm is also increases. In this paper, we propose a method based on Discrete Cosine Transform (DCT) in order to improve time complexity. The proposed technique can also detect forgery even after some post processing operations such as rotation and Gaussian noise addition.

Keywords
Copy-move forgery; Discrete Cosine Transform(DCT); Block matching; passive forgery detection; image forgery

1. INTRODUCTION
The authenticity of digital images has a Fundamental need of many areas, including: forensic investigation, criminal investigation, insurance processing, surveillance systems, intelligence services, medical images and journalism. But, in today's digital world, it is very easy to create, alter and modify the information depicted by an image without leaving any visual evidence of tampering. This is mainly because of the existing powerful digital image technologies. Despite this, there is no such system exists which can detect forgery efficiently and correctly.

1.1 Categorization of image forgery
Detection of image fakery is used to verify the integrity of digital images. The integrity of image can be verified by two methods.
(1)Active or intrusive
(2) Passive or blind
Active method requires some known information to be added in the original image. Authenticity of such
Images can be verified by comparing the code obtained from the image with the original embedded information. Watermarking and digital signature are some examples of active method. So before the distribution of the image this method requires dedicated hardware or software to embed the authentication code inside the original image.
On the other hand, passive method does not require any prior embedding of information in the original image. It is based on the fact that, some specific statistical properties of an image are highly disrupted when an attempt of tempering is made. This leads to introduction of various inconsistencies in the image. These inconsistencies are strongly used to detect the forgery. This is a very popular technique because it does not require any prior knowledge about the image [4].

1.2 Workflow Structure of Forgery Detection Techniques
Passive detection techniques take every image as a forged or tempered image. After performing a particular series of operations the image is classified into two categories: authentic images and forged images. We describe here a common workflow structure of passive image forgery detection techniques in Fig.1 which comprises the following steps:

(1) Image preprocessing: In this first step some preprocessing operations are performed on the image. As most of the method require gray scale images so the colored image is first converted into a gray-scale image. Then some other necessary operations like cropping and frequency domain transformations like DCT or DWT are also performed to enhance future processing. This step is common in both the block-based methods and key-point based methods.

(2) Feature extraction: In this step a set of sensitive features (like color, texture, edge etc.) are extracted for each part of the image. These features are mainly used to distinguish each part from all others. Several methods are used for feature extraction: frequency domain, transform based, or spatial domain. After extraction these features are stored in a feature vector. To reduce the computational complexity of the detection algorithm, constructed feature vector should be of low dimension [1-6].

(3) Matching: After feature extraction feature vectors are sorted so that the most similar feature vectors appear in consecutive rows. For block-based methods most researchers use lexicographic sorting. Whereas some other use k_d-tree method to find approximate nearest neighbors. k_d-tree method is mostly used in key-point based algorithms. It has been shown that k_d-tree approach is better than the lexicographic approach but the memory requirement for k_d-tree is significantly higher [4].

(4) Filtering: Filtering methods are used to increase the probability of correct matches and also to reduce the probability of false matches. Euclidean distance is used by most of the algorithms between matched feature vectors. As neighbor pixels have similar features which may be leads to false matching. Bravo-Solorio and Nandi proposed an algorithm in which correlation coefficient is used as matching factor between two feature vectors. The purpose of this step is to categories images into two categories: original and forged images.

(5) Post processing: This step mainly checks the accuracy of the technique against some common image post processing operations such as rotation, scaling and JPEG recompression and used to localize the exact forged region in the image.

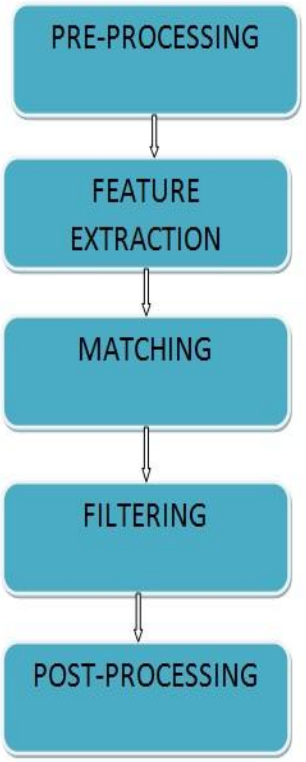

Fig.1: Workflow structure of forgery detection techniques

2. PROPOSED METHOD

2.1 Algorithm Framework

In our algorithm, we first divide the original image into fixed size overlapping blocks and then determine the uniqueness of those blocks and then output the forged parts as shown in Fig.2. Details are as follows:

Step 1: Assuming a X×Y grayscale image (if the image is a color image then we have to use the following standard formula: I = 0.228R + 0.587G + 0.114B in order to change it into grayscale), we first divide it into overlapping blocks of P×P pixels, that is, the neighboring blocks have only one different column or row.

Each block is r epresented by P_{ij}, where i and j represents the starting point of the block's row and column, respectively.

Hence we are able to obtain NOB of overlapped sub-blocks from suspicious image.

$$NOB = (X - P + 1) \times (Y - P + 1) \quad (1)$$

Step 2: For each block DCT is performed. Then a DCT coefficients matrix of the same size as of the block is created.

Step 3: As each block is denoted by the DCT coefficients, here we use the size of the block is 8 × 8; the size of the coefficient matrix is also 8 × 8, so there are 64 coefficients in the matrix. As it is the nature of DCT that the energy only focuses on the low energy coefficients, that is not all the elements are important, only the low energy coefficients play the crucial role in the detection process. Coefficients are selected in a zigzag order.

Step 4: We extract the low energy DCT coefficient in a zigzag manner. It corresponds to only ¼th energy of the entire DCT coefficients. Then we divide that extracted low frequency part into four sub-parts S_1, S_2, S_3, S_4, and calculate the mean of DCT coefficients of each sub-part. In order to obtain the features for matching, we use A_1, A_2, A_3 and A_4, as the obtained feature of S_1, S_2, S_3, S_4 respectively. We can get A_i (i= 1, 2, 3, 4) through equation 2.

$$A_i = \frac{\sum f(x,y)}{4}, \left(f(x,y) \in S_i, i = 1,2,3,4 \right) \quad (2)$$

Where A_i represent the mean of the coefficients value, related to each S_i. Since each S_i is represented by different DCT coefficients and which can represent the energy of the image. After that, four features are obtained, which can be combined to form a feature vector of size of 1×4, denoted as:

$$V_i = [A_1, A_2, A_3, A_4] \quad (3)$$

Step 4: The feature vectors extracted from step 3 are arranged to a matrix, denote as A with the size of (X-P+1) (Y-P+1) × 4.

$$L = \begin{bmatrix} V_1 \\ V_2 \\ . \\ . \\ V_{(X-P+1)(Y-P+1)} \end{bmatrix} \quad (4)$$

The L is then sorted lexicographically, in the meantime, record each block's left corner's coordinate. Based on A, the Euclidean distance match (L_i, L_{i+j}) between neighboring pairs of L is obtained. If the distance is smaller than a preset threshold DS, then that block is considered as a pair of candidates for the forgery.

$$L_i = \left(A_i^1, A_i^2, A_i^3, A_i^4 \right) \quad (5)$$

$$L_{i+j} = \left(A_{i+j}^1, A_{i+j}^2, A_{i+j}^3, A_{i+j}^4 \right) \quad (6)$$

$$Compare\left(L_i, L_{i+j}\right) = \sqrt{\sum_{k=1}^{4} \left(A_i^k - A_{i+j}^k \right)^2} < DS \quad (7)$$

In addition, according to the fact that the neighboring blocks may have the similar feature vector, we calculate the true distance between two identical blocks as follows:

$$dist\left(V_i, V_{i+j}\right) = \sqrt{\left(x_i - x_{i+j}\right)^2 + \left(y_i - y_{i+j}\right)^2} > ND \quad (8)$$

Here (x, y) is the starting coordinate of the blocks. Equation (7) and (8) are used to determine whether the blocks are forged or not.

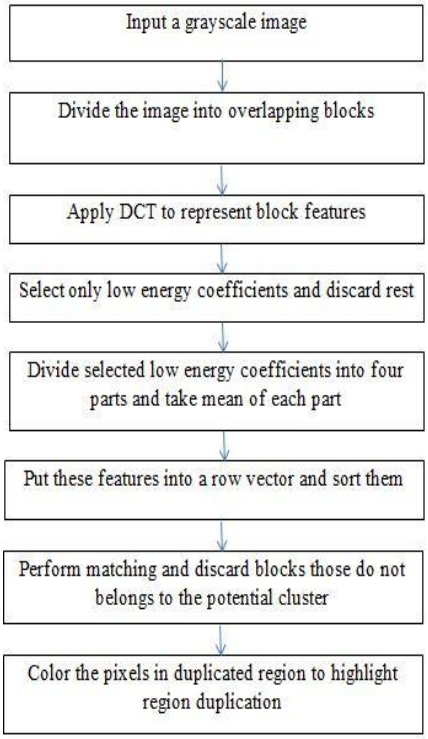

Fig.2: Algorithm structure

In a nutshell, in order to make the detection, four thresholds have been set: the overlapping window B, similarity threshold DS, distance threshold ND, and N_{num} which controls the amount of neighboring feature vectors, only if the test satisfies the following condition:
Compare (V_i, V_{i+j}) < DS & dist (V_i, V_{i+j}) > ND

Step 5: This is the last step of the algorithm, in this step both, the original and the duplicate regions are marked with black color in order to highlight the forged region.

3. EXPERIMENTAL ANALYSIS AND RESULTS

We conducted a number of experiments using the proposed method to detect copy-move forgery with a large number of images. For experiments, we used Matlab 8.1.0.604 (R2013a) in 64-bit system to complete the experiments by proposed method. The hardware specification was Intel i5 2.5 GHz processor with 8 GB DDR3RAM. The performance of the proposed system is given in terms of accuracy in Equation (9)

$$Accuracy = \frac{T_p + T_n}{T_p + T_n + F_n + F_p} \times 100 \qquad (9)$$

Where:

- **T_p (True Positive)** is the number of forged images, which are classified as forged images.
- **T_n (True Negative)** is the number of authentic images, which are classified as authentic images.
- **F_p (False Positive)** is the number of authentic images, which are classified as forged images.
- **F_n (False Negative)** is the number of forged images, which are classified as authentic images.

These measures are calculated in blocks rather than pixels. If more than 50% area of a block is under copy-move attack, that block is considered as forged block. The performance of the proposed method is compared with two other related methods that are described in [1] and [3]. In [1], the authors use all the 64 quantized DCT coefficients for matching, while in [3], the authors use only 16 low energy DCT coefficients to detect copy-move forgery.

Table 1 Computational Complexity Comparison

Literatures	Extraction method	Feature dimension
[1]	DCT	64
[2]	PCA	32
[3]	DCT	16
Proposed	DCT	4

According to the information represented by the TABLE I the prior methods have a large feature vector dimension as compare to the proposed method which uses only four features to represent a block. The number of the overlapping blocks is same as in the previous methods but, the feature vector's dimension of the proposed method is lower, which implies that the proposed method has a lower computational complexity as compared to the previous methods.

To compare the robustness and speed of the proposed algorithm with the existing methods, a database of 100 images is developed. The database consists of images with different contrasts and resolutions. To test the robustness of the proposed method against added noise forged images of Signal to Noise Ratio (SNR) ranging from 90 to 40 db has taken. Block size is also varied from 4 to 16 but the algorithm shows the best results with the block size 8, so we only use 8 as block size in our results.

In the first case, a low contrast image is shown in Fig. 3. In this image the bulb is copied in the same image to increase the redundancy. The proposed method successfully locates the copied and the pasted region and colors both of them as black to highlight it.

In Fig.4 a high contrast image, in Fig.5 a low resolution image and in Fig. 6 a high resolution image is shown. It revealed that the proposed method is faster than the existing methods. Thus, the proposed algorithm is the advanced version of the DCT-based block matching algorithms.

The proposed method detected the forgery with 100% success rate for SNR above 50 db. The success rate comes down to 85% for SNR below 40 db and the accuracy comes down to less than 50%. Also the efficiency of the proposed method is highly dependent upon the size of copy-moved region.

The threshold setting in the proposed method is purely on the experimental basis and the setting of threshold varies from image to image. For our experiment we have taken the image size 256 × 256 and type of image is grayscale image. If the images are color images then it must be converted into the grayscale image.

In the proposed method we have to set the threshold DS and ND. DS is set to 0.4 and ND is set to 25. DS, is used to determine whether two blocks are identical or not. If the value of Equation (7) is less than DS then these blocks are

considered as the candidate blocks for the copy move forgery detection.

After this, the Equation (8) is used to detect the actual distance between the candidates blocks, if the value of Equation (8) is greater than N_d then the blocks are confirmed as the part of copy-move forgery, otherwise it is discarded. So, the setting of these two thresholds is very crucial in order to efficient detection of duplicated regions in the forged image.

Table 2. Performance Comparison

Name of Image	Running Time (in sec.) of DCT method	Running Time (in sec.) of I-DCT method	Running Time (in sec.) of Proposed method
Image1(Low Contrast)	23.12	20.10	18.25
Image 2(High Contrast)	18.92	15.32	11.69
Image 3(Low Resolution)	7.23	6.12	4.36
Image 4(High Resolution)	39.74	34.57	30.46

The above comparison shows that the proposed method is far better than the existing two mostly used methods.

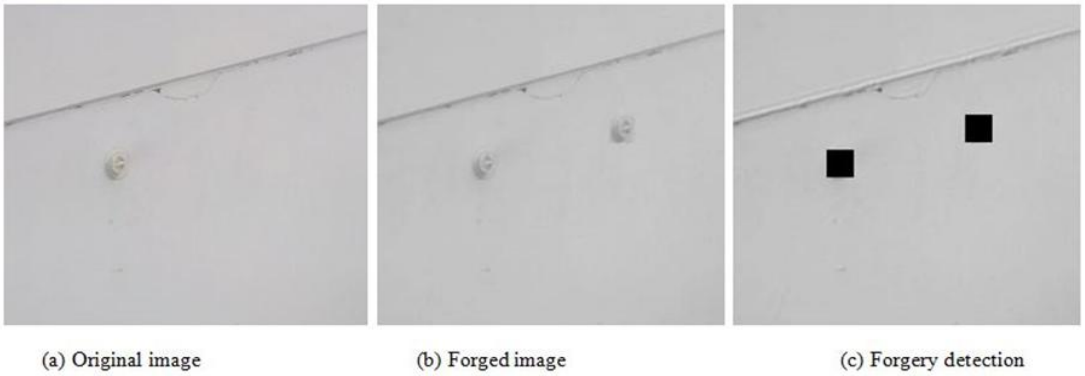

Fig.3: Copy-move forgery detection in a low contrast image

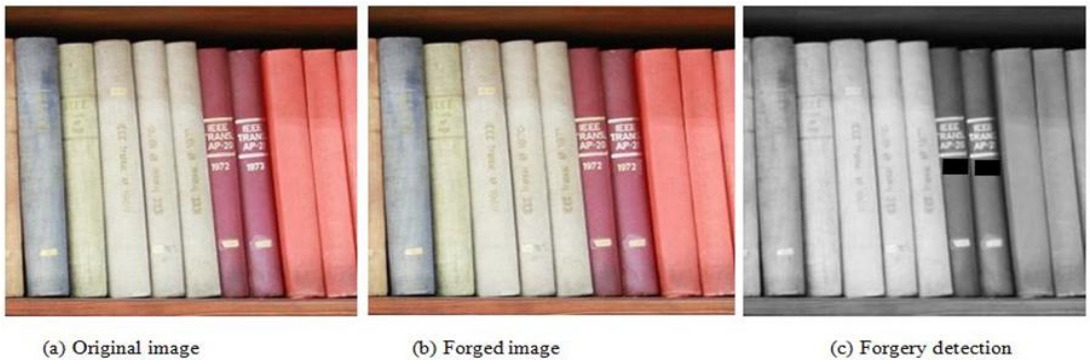

Fig.4: Copy-move forgery detection in a high contrast image

Fig.5: Copy-move forgery detection in a low resolution image

(a) Original image (b) Forged image (c) Forgery detection

Fig.6: Copy-move forgery detection in a high resolution image

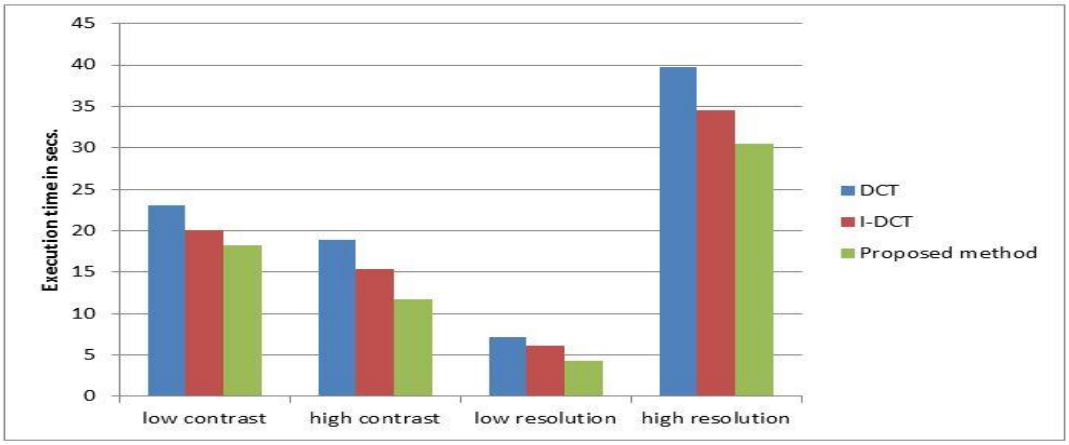

Fig.7: Execution time comparison

4. CONCLUSIONS

We have presented here an effective and efficient algorithm based on DCT to detect copy move forgery. The proposed method has a less feature vector dimension as compared to previous works [1, 3]. The

experimental results and analysis shows that the proposed method detect forgery not only accurately but also detects it in a less amount of time as compared to the previous work [1, 3].

Also, it has shown a good success rate against JPEG compression, added Gaussian noise and a

small amount of rotation and scaling. The proposed algorithm is the improved version of the existing block matching algorithm based on DCT with improved time complexity.

5. REFERENCES

[1] Fridrich, J., Soukal, D., and Lukas, J. 2003 Detection of copy-move forgery in digital images In: Proc. of digital forensic research workshop.

[2] Popescu, A.C., and Farid, H. 2004 Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515, Department of Computer Science, Dartmouth College.

[3] Huang, Y., Lu, W., Sun, W., and Long, D. 2011 Improved DCT-based detection of copy-move forgery. In images forensic science international, vol. 206.

[4] Birajdar, G.K.., and Mankar, V.H. 2013 Digital image forgery detection using passive techniques: A survey. In Digital investigation, vol. 10, no. 3.

[5] Mahdian, B., and Saic, S. 2007 Detection of copy-move forgery using a method based on blur moment inverients. In forensic science international, vol. 171, no. 2.

[6] Cao, Y., Gao, T., Fan, L., and Yang, Q. 2012 A robust detection algorithm for copy-move forgery in digital images. In forensic science international, vol. 214.