Enhanced Passive Copy – Paste Tampering Detection Technique for Digital Images

AR. Guru Gokul
Assistant Professor
Department of Computer Science and Engineering
Sri Krishna College of Technology, Coimbatore

N. Kumaratharan
Professor
Department of Information Technology,
Sri Venkateswara College of Engineering, Chennai.

P. Suguna
Assistant Professor,
Department of Information Technology,
Roever College of Engineering and Technology, Perambalur.

ABSTRACT
Digital images are powerful and widely used communication medium in many fields like medical imaging, digital forensics, surveillance, journalism, etc. The availability of sophisticated digital image technology has given rise to image forgery. The forgeries are very difficult for a human eye to detect. Passive tampering detection method aims to detect the tampering areas in the digital images without any prior knowledge of the original images. The available tampering detection technique uses 8 x 8 blocks to detect the tampered region. However, all the pixels involved in the block are not compared, which again leads to a forgery. To mitigate these effects, a new progressive passive copy-paste tampering detection technique is proposed. Experimental result shows that the proposed technique overcomes the foresaid technique which enhances the tampering detection method.

Key words – Image Forgery; copy-paste forgery; JPEG; Quality factor

1. INTRODUCTION
The digital images are a powerful medium of communication with large amount of information. Today's images have an important impact on the society. The image authentication and verification is important that are used in many fields such as forensic investigation, criminal investigation, surveillance systems, and intelligence services [1]. Using the various software that are available today, the digital images can be forged without leaving any traces.

The JPEG format uses lossy compression which sacrifices image quality for file size. Lossy compressed images discard pixels that should not degrade image quality for a greater extent, based on a configurable quality factor. In [3], the *blocking artifact grid* (BAG) method was proposed to detect doctored JPEG images. In [3], Luo et al. presented *blocking artifact characteristics matrix* (BACM), which exhibits regular symmetrical shape for original JPEG images, and applied it to expose digital forgeries by detecting the symmetry change of BACM.
Barni et al. [2] proposed two algorithms for detection of copy-paste tampering by means of double JPEG detection and image segmentation, but both of them are time-consuming and segmentation of the tampered images were difficult. Lin et al. [5] developed a method for detecting tampered JPEG images by examining the double quantization effect hidden among the DCT coefficients, and computing the block posterior probability map by bayesian approach. Copy-move forgery detection methods presented in [6-8] are only effective when a part of the image is copied and pasted into the same image.

Performing statistical calculations on the boundaries of these blocks builds upon the technique presented by Fan and Queiroz [9] for detecting prior JPEG compression in a BMP image. These copy-paste operations introduce small anomalies in the statistical data of the newly created forged JPEG image. Therefore, the proposed tampering detection method analyzes a JPEG image with respect to the *2 x 2* blocks used by the JPEG compression scheme.

2. METHODOLOGIES
2.1 Image Tampering Scenario
Every image has different quality (compression ratio) factor. In copy-paste tampering the tampered image has two different quality factors. For example consider the Fig. 1, the image-A has quality factor Q-A, image-B has quality factor Q-B. The part of image-B is copied and pasted into image-A. The tampered image is image-C.

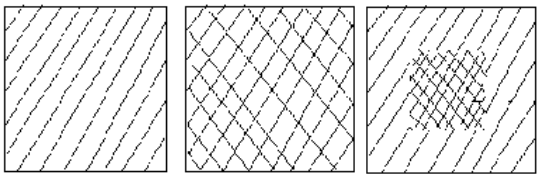

Fig. 1: Example of copy-paste tampering in terms of JPEG compression ratio (Quality factor)
(a) Image-A with quality factor Q-A
(b) Image-B with quality factor Q-B
(c) Image-C (Tampered image)

The image-C has two different quality factors, which are Q-A (Quality factor of image-A) and Q-B (Quality factor of image-B). These different quality factors are used to detect the tampered area in the image.

2.2 Tampering Detection Method
If two images are used to create a forgery, it is likely that both have different levels of compression, specifically the "Quality Factor". Also, it is likely that resizing, rotating, or cropping was performed on the tampered portion to ensure it blends in with the rest of the image.

The tampered image's authenticity is more believable and the forgeries are very difficult for a human eye to detect. These copy-paste operations introduce small anomalies in the statistical data of the newly created forged JPEG image. Therefore, the proposed technique to detect tampering analyzes a JPEG image with respect to the *2 x 2* blocks used by the JPEG compression scheme. Fig. 2, shows an abstract representation of a 2 x 2 block of pixels in a JPEG image with letters representing interested pixel values.

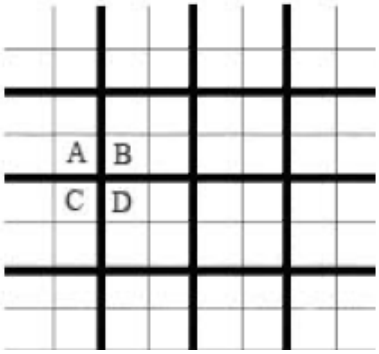

Fig. 2: Abstract representation of a 2 x 2 block

The following result is calculated based on the numerical pixel values at locations A, B, C, and D in every *2 x 2* block, (*i, j*) , which makes up the image (see Figure 2):

$$R(i, j) = |A-B-C+D|$$

The R(i,j) represents the pixel variation between the three neighbor pixels of another blocks in the image. Creating a forged JPEG image from portions of two other JPEG images, with different quality factors or having been cropped, rotated, or rescaled, introduces anomalies in the average *R*(*i, j*) values across the image. The *R*(*i, j*) value obtained using above formula of each *2 x 2* pixel blocks of a forged image is used to determine the statistical anomalies in the tampered areas. All *R* (*i, j*) values can be calculated for each *2 x 2* block and then analyzed by some limit of threshold values. After calculating the pixel variation of each block, the following formula is used to find limit of threshold value,

Max = maximum (R (i, j))
Min = minimum (R (i, j))
Limit_start = 0
Limit_end = (Max + Min)/3
Threshold limit = Limit_start to Limit_end

The difference here is that all 4 pixels in each *2 x 2* block will be either entirely white or black based on the value obtained from the following formula:

$$Dright\ (i, j) = |R\ (i, j) - R\ (i, j+1)|$$
$$Dbottom\ (i, j) = |R\ (i, j) - R\ (i+1, j)|$$

The threshold values are used to produce binary image. Here, *Dright* (*i, j*) equals the difference between a block's *R* (*i, j*) value and its direct neighbor to the right's value. *Dbottom* (*i, j*) equals to the difference between a block's *R* (*i, j*) value and its direct neighbor to the bottom's value. Blocks at the far right and bottom edge of an image get *Dright* (*i, j*) and *Dbottom* (*i, j*) values equal to zero as this should not be an area of interest for tamper detection. Therefore, they are effectively ignored.
Once all *Dright* (*i, j*) and *Dbottom* (*i, j*) values are calculated, compare *Dright* (*i, j*) and *Dbottom* (*i, j*) with each threshold value. The threshold value is used to set all blocks equal to white if their *Dright* (*i, j*) or *Dbottom* (*i, j*) value is equal to or greater than threshold value. Otherwise, it is set to black. Each threshold value produces different binary image. By performing OR operation with all binary images, the output is produced. The binary image has only white and black pixels. The binary image shows the tampered areas in the forged image. The white pixels present in the binary image represent the tampered area and black pixels in the binary image represent the original area in the image.

3. ENHANCED COPY – PASTE TAMPERING DETECTION METHOD

3.1 Enhanced Copy – Paste Tampering Detection Method

The existing tampering detection method uses 8 x 8 blocks to identify the tampered region. Hence, many pixels are not compared during the detection process. To overcome this drawback, in the proposed enhanced copy – paste tampering detection method 2 x 2 blocks are used to identify the tampered region. The proposed system model consists of the following steps:

Step 1: The color image is converted into a grayscale image

Step 2: The gray scale image is divided into 2 x 2 blocks

Step 3: Statistical analysis are performed on the 2 x 2 blocks.

Step 4: Based on the threshold value,

Step 4 a: If 2 values are similar, a black pixel is set.

Step 4 b: If 2 values are different, a white pixel is set.

Step 5: Display the tampered region.

The proposed system model is represented in Figure 3 as follows:

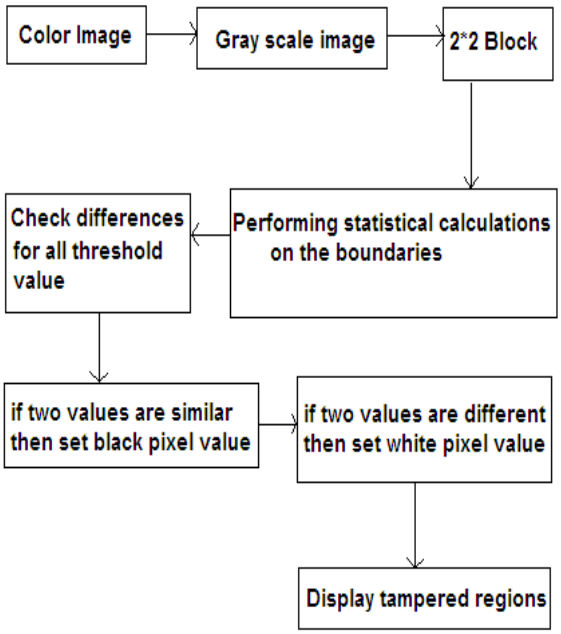

Fig. 3: Enhanced copy – paste Tampering Detection Method

3.2 Proposed Enhanced Tampering Detection Method

The proposed enhanced copy-paste tampering detection method consists of the following steps:

1) Convert color image into grayscale image
2) Divide image into 2 x 2 compression blocks (i , j)

3) Find degree of pixel variation present between an 2 x 2 block and its 3 neighbors for each 2 x 2 JPEG compression block (i , j) within bounds
R (i, j) =| A−B−C+D| where
A = pixel value (2*i, 2*j) in image,
B = pixel value (2*i, [2*j] + 1) in image,
C = pixel value ([2*i] + 1, 2*j) in image,
D = pixel value ([2*i] + 1, [2*j] + 1) in image End
4) Find threshold limit
5) Perform Comparison operation for each threshold value t for each 2 x 2 JPEG compression block (i , j) within bounds
Dright (i, j) = |R (i, j) − R (i, j+1)|
Dbottom (i, j) = |R (i, j) – R (i+1, j)|
end
for each 2 x 2 JPEG compression block (i , j) within bounds
if (Dright (i, j) ≥t) OR (Dbottom (i, j) ≥t)
set all pixel values in (i , j) to white
else
set all pixel values in (i , j) to black
end
6) Perform OR operation between previous binary output with current binary output
end

The block size is taken as 2 x 2 in the proposed technique. The existing system uses a block size of 8 x 8, where many pixels are not compared because of the larger size of block. In the proposed method, every pixel is compared and tampered region is detected effectively.

4. EXPERIMENTS AND DISCUSSION

The proposed method is applied to many images and the performance of the algorithm is evaluated. Two types of images set are used in the experimentation.

- Manual forged image sets.
- CASIA Tampered Image Detection Evaluation Database (CASIA TIDE v1.0).

4.1 Manual Forged images

This type of image sets are created using Photoshop image editing software tool. Totally 15 tampering images are created using image editing tool. Each image has different size. The proposed method is applied to all tampered images and the time taken for evaluation is recorded.

A color image is manually tampered and the tampered image is given as input to the system. The tampered regions are effectively revealed in the output binary image. The sample set of output is shown below:

Fig. 4: Evaluation for manual image (a) The original image (b) The tampered image given as input (c) The binary image shows the tampered regions.

4.2 CASIA Tampered Image Detection Evaluation Database (CASIA TIDE v1.0)

CASIA TIDE v1.0 is one type of authenticated image sets. The dataset contains authenticated and spliced color images of size 384x256 pixels in JPEG format. The authentic images were mostly collected from the Corel image dataset and others are taken by our own digital cameras. The sample set of output using the image from CASIA TIDE v1.0 is shown:

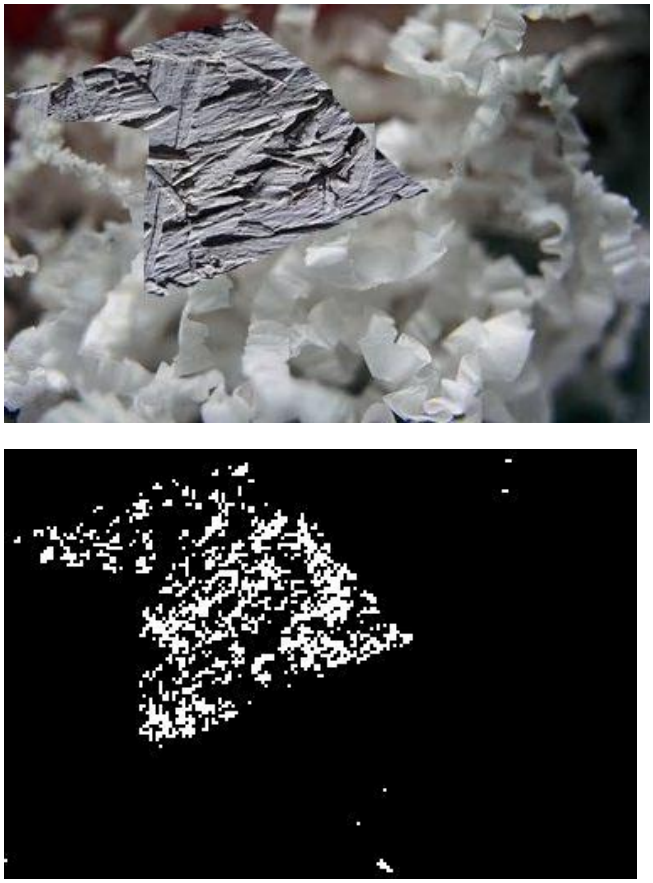

Fig. 5: Evaluation for CASIA image (a) The original image (b) The tampered CASIA image given as input (c) The binary image exposing the tampered regions

All tampered images in this database are made only by splicing operation. Spliced images are generated from authentic images by crop-and-paste operation using Adobe Photoshop CS3 version 10.0.1 on Windows XP. Spliced region(s) are either from the same authentic image or from another image.

A sample tampered image from the CASIA database is given as input to the proposed algorithm and the output generated are observed. Various set of outputs are compared to evaluate the performance of the proposed algorithm. The sample output using the image from CASIA database is shown in Figure 4.

To further confirm the validity of the proposed algorithm, various images of different size are given as input and the corresponding evaluation time is recorded in the Table 1. The results shows that the evaluation time is decreased and the results are more accurate than the older methods.

Table 1. Time taken for the proposed algorithm for identifying the tampered regions in different images

Image Size	No. of Images	Avg. Time (sec)
1024 x 728	4	11.18538425
259 x 194	5	0.7019296
800 x 600	5	5.597219
3472 x 2604	1	297.811226

5. CONCLUSION AND FUTURE WORK

The digital image forgery and image authentications are main issues in forensic system. The tampering in digital image is difficult to detect by human eye. The proposed method for JPEG compression analysis technique is more effective to detect the copy-paste tampering without using original image. The JPEG compression analysis is one of the blind methods, which is effective in detecting any changes. The method is applied to many images such as manual forged image set and CASIA TIDE v1.0 image set and the method effectively detects the tampered area in the different forged images. Experimental results show that the performance of the proposed method and effectiveness for detecting the tampered area in digital images. The image tampering detection leads to lot of applications such as forensics, surveillance and journalism etc. One of the issues of this algorithm is that the tampering detection is little tougher in the case when both original and the tampered region have the same quality factor.

6. REFERENCES

[1] B. Mahdian, S. Saic. "A bibliography on blind methods for identifying image forgery", Signal Processing: Image Communication, 25(6): 389-399, 2010.

[2] M. Barni, A. Costanzo, L. Sabatini. "Identification of cut & paste tampering by means of double-JPEG detection and image segmentation", Proceedings of 2010 IEEE International Symposium on Circuits and Systems, Paris, France, pp. 1687-1690, 2010.

[3] W. Li, Y. Yuan, and N. Yu. "Passive detection of doctored JPEG image via block artifact grid extraction", Signal Processing, 89(9): 1821-1829, 2009.

[4] Z. Lin, J. He, X. Tang, and C. K. Tang. "Fast, automatic and finegrained tampered JPEG image detection via DCT coefficient analysis", Pattern Recognition, 42(11): 2492-2501, 2009.

[5] W. Luo, Z. Qu, J. Huang, and G. Qiu. "A novel method for detecting cropped and recompressed image block", IEEE International conference on Acoustics, Speech and Signal Processing, 2: II- 217-II-220, 2007.

[6] J. Fridrich, D. Soukal, and Jan Lukáš. "Detection of copy-move forgery in digital images", Proc. Digital Forensic Research Workshop, Cleveland, OH, USA, 2004.

[7] B. Mahdian, and S. Saic. "Detection of copy–move forgery using a method based on blur moment invariants", Forensic Science International, Vol. 171(2), Pages: 180-189, 2007.

[8] S. Bayram, H. T. Sencar, and N. Memon. "An efficient and robust method for detecting copy-move forgery", IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1053-1056, 2009.

[9] Fan, Z. and R. L. de Queiroz, "Identification of Bitmap Compression History: JPEG Detection and Quantizer Estimation", IEEE Transactions on Image Processing, Vol.12, No.2: 230-235, February 2003.

[10] CASIA Tampered Image Detection Evaluation Database, CASIA TIDE V1.0, http://forensics.idealtest.org:8080/index_v1.html.