Tamper Detection and Identification of Cropped Blocks in JPEG Images

Athulya B
Department of Computer Science
College of Engineering, Karunagapally,
Kollam, Kerala

Manoj Ray D
Department of Computer Science
College of Engineering, Karunagapally,
Kollam, Kerala

ABSTRACT

In this paper a detailed study regarding Digital Image Forgery on Jpeg images is provided. Here, copy-paste block detection on a special case of double Jpeg compression - Shifted Double Jpeg Compression, is identified based on the characteristics of Double Jpeg compression. In certain cases the tampered image will be cropped, the paper uses properties of Block Artifacting method to identify such a scenario.

General Terms

Digital Image Forgery, Copy-paste block detection, Shifted Double Jpeg Compression, Block Artifact.

1. INTRODUCTION

Digital images and videos, being used in for wide purposes, carry an important role in today's technical world. As its uses increases, fraudulent methods were also developed for tampering which diminishes the credibility of these images and videos. Many methods were introduced to prevent tampering - Water Marking systems were a successful method amongst them. Water marking system acted as a means to authenticate the contents of the digital image. But there were limitations to this method too. There existed cases were water marking system can't be applied, such as on images or videos from surveillance cameras, military cameras etc. To overcome such scenarios, pioneers carried out researches which involved detection of tampering caused to a digital image.

Fridrich et al.$^{[1]}$ presented methods, in order to detect tampering, for camera identification based on the identification of pattern noise of the sensors in digital cameras and copy-move forgery based on pixel matching. Farid and Popescu developed several statistical methods in order to detect forgery, based on re-sampling [2] and color filter interpolation [3].

Lukas et al .[4] proposed block matching method that checks each block of the tampered image with that of the original image so as to detect the tampering. NG and Chang [5] developed a physics based model for distinguishing computer graphics from natural images and proposed another method to detect photomontage by image spicing.

One of the most commonly used image compression format is Jpeg. Jpeg compression standard has been widely used in most of the internet applications. Therefore tamper detection in Jpeg images can play an important role in countering image forgery. Most of the recent researches have been developed based on double compression of Jpeg images - identifying image that have undergone compression twice. A possible solution to this problem was presented by Lukas and Fridric [4] by estimating the primitive quantization table from a double compressed Jpeg image directly. Tampering in Jpeg images results in a change of original compression factor due to occurrence of recompression. Although these methods work on different principles they have restrictions and drawbacks. In the following subsection these drawbacks and limitations are briefly summarized.

Copy-paste tampering is most commonly seen since it is easy to perform. An example is shown below:

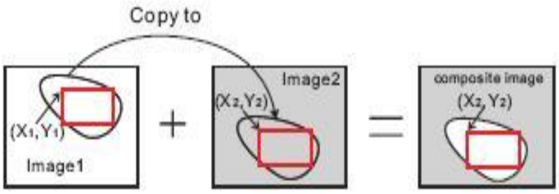


Fig 1: Composite image

Above figure shows how a typical copy-paste forgery can be performed. The Process consists of copying a part of the image and pasting it on the target image. The copied portion can either be from the same image or else it can be from different image, and the process is carried out in order to hide any information or fabricate any portion of the image. This can be done with such perfection that even bare eyes won’t be able to identify.

1.1 Quantization Table Inconsistencies

In a Jpeg encoder, before encoding, all the 8x8 Discrete Cosine transform (DCT) blocks will be quantized by same quantization matrix. Once a Jpeg image is tampered using copy move forgery, the tampered image may inherit characteristics of different source's quantization table and thus may result in inconsistencies. In [6], the quantization table is estimated by quantization error minimization. In [7] and [8] Maximum likelihood estimation [7] and MAP approach [8] are proposed to achieve Jpeg quantization steps.

1.2 Compression Artifact Abnormalities

When a tampered Jpeg image is double compressed - when it is recompressed and saved again in Jpeg format, the final image will have different compression properties than that of single compressed images. This difference in the blocking artifacts is used to detect recompression in Jpeg images. However in cases where there are misaligned blocks boundaries, then this method can't be used to detect abnormalities.

1.3 Non Perfect Histograms

Despite the advantages of the method presented in [10], certain experiments discovered that there are some drawbacks in this method.

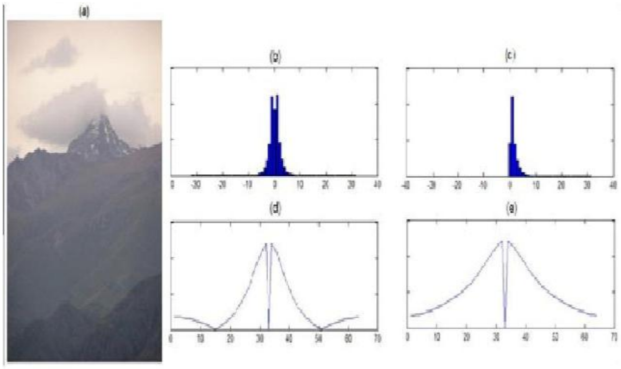


Fig 2: Shows (a) the tested single compressed images; (b),(d) outputs of the above method resulting in a false positive (the spectrum has not the typical decaying trend); (c),(e) output of the method described in this paper. In both cases the method was applied to DCT coefficients for same frequency

For example, applying the method to natural images with "non-perfect histograms" (histograms which have not a well decaying trend or histograms which being not perfectly approximated by a Gaussian or Laplacian) causes false positives (single compressed imaged classified as double compressed). It was noticed that the number of false positives is rapidly increasing when the method is applied to "un-natural" images (for example, scanned paper forms). Furthermore, application of a machine learning-method such as SVM improves the method's results.

The rest of the paper is organized as follows: Section II gives some preliminary results about JPEG compression, Double Compression and Shift Double JPEG compression (SDJPEG). In section III, we join another technique block artifacting method as an extension. Lastly, in Section IV, we conclude the paper.

2. PRELIMINARIES

In this section, a brief explanation of JPEG methodology and Double compression is given.

2.1 JPEG Algorithm

JPEG is one of the most commonly used compression format(i) and it provides better compression ratio. The algorithm is quite simple; the entire image is initially divided into 8x8 blocks. Each of these blocks is transformed by forward DCT(ii) into a set of 64 values referred to as DCT coefficients. The upper left most corner value is referred to as the DC (Direct Current) and rest of the 63 values are said to be the AC (Alternate Current) value. After applying DCT, since it is a lossy compression, quantization will be applied. Based on each quality factor quantization matrix varies. After which entropy encoding is performed.

JPEG committee has developed a standard quantization matrix for 50% Quality factor

$$\text{std\_quant} = \begin{pmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{pmatrix}$$

For rest of the quality factor we use,

$$\text{Im\_qtable} = (\text{std\_quant}*S+50) \div 100$$

if the quality factor Q, is greater than 50% then,

$$S=5000\div Q$$

Otherwise,

$$S= (200-2)*Q$$

Trade-off between visual quality and compression rate can be achieved by using a proper quality factor.

2.1 Double Compression

When a compressed image is resaved again in JPEG format after performing some manipulation, then that is double compression. In more simple words, saving an image twice results in double compression.

During the JPEG compress, each DCT coefficients c is then quantized by an amount *q*, *c=c/q*, where *q* depends on the quality factor. Consider now a set of coefficients c_1 quantized by an amount q_1, which are subsequently quantized a second time by an amount q_2 to yield coefficients c_2. With the exception of $q_2 =1$ (i.e., no quantization), the difference between c_1 and c_2 will be minimal when $q_2 = q_1$. It is obvious that the difference between c_1 and c_2 increases for a quantization value $q_{2>}q_1$ since the coefficients become increasingly more sparse as q_2 increases. For values of $q_2 < q_1$, the difference between c_1 and c_2 also increases because although the second quantization does not affect the granularity of the coefficients, it does cause a shift in their values [9].

Double compression can occur in two ways:

Simple double compression where the image is resaved in order to compress more. This need not necessarily involve any tampering.

Second one will be situation where image will be resaved after performing copy-paste tampering on the image. This scenario is termed as Shifted Double JPEG compression (SDJPEG) in [9].

The main property of double JPEG compression is that it brings out a detectable effect like periodic zeros and double peaks.

3. DETECTING TAMPERED AREA

This consists of two portions. First involves whether the image is double compressed or not and then tampering is checked finally, tampered region is marked.

3.1 Detection of Copy-paste Tampering

According to the above, the quantized DCT coefficients differ from the original coefficients in that the quantized DCT coefficients is related to the quantization matrix **Q** the quantized DCT coefficients has been standardized by the quantization matrix **Q** so in DCT block, every element in the quantized DCT coefficients can be divided by corresponding figure in **Q**, but the original coefficients don't have such characteristics [9]. But in the case of images which suffered compression twice, the coefficients depend on primary **(Q_1)** as well as secondary quantization matrix (**Q_2**). Right margins should be justified, not ragged.

We quantize the quantized DCT coefficients of the double compressed image by an amount of quantization matrix **Q_i** separately to detect this characteristic. The image has now experience JPEG compress three times, the original DCT coefficients **C_0** is quantized by **Q_1** to yield **C_1** then **C_1** is quantized by **Q_2** to yield **C_2**, and finally **C_2** is quantized by different **Q_i** to yield **C_{3i}**. As before, the difference between **C_{3i}** and **C_2** will be minimal when **$Q_i = Q_2$**, or **Q_i** is a matrix whose elements are all 1. And since the coefficients were initially quantized by **Q_1**, we expect to find a second minimum when **$Q_i = Q_1$**. According to this, we can detect whether a JPEG image is double-compressed [9].But in the case of SDJEPG, certain modification to the above method has to be done.

When the JPEG image undergoes copy-paste tamper the primary quantization factor or quantization factor of original image ***O*** is p_1 and the quantization factor of inserted image ***I*** is p_2 and the quantization factor of the final image ***D*** is p2.The entire image is divided into 8x8 or 16x16 blocks *B(x, y)*. As mentioned earlier, each of these blocks *B(x, y)* will be quantized with matrix **Q_i** where **Q_i** depends on various quality factor p_i, after performing DCT. Let the DCT coefficients of B(x, y) be *C(x, y)* and the corresponding quantized DCT coefficients be represented as $C_i(x, y)$ then the difference between *C(x, y)* and $C_i(x, y)$ can be calculated as:

$$\text{dif}(x, y, p_1)=1/3\left(\sum_{m=1}^{M}\sum_{n=1}^{N}\sum_{k=1}^{3}\left\|B(m,n,k)-Bi(m,n,k)\right\|\right)$$

Where (*M*, *N*) is the size of the Block, *B* (*m, n, k*), *k*=1, 2, 3 stands for the DCT coefficients value of the RGB channel.

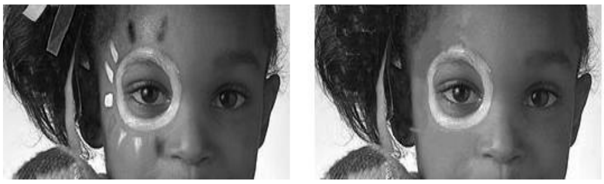
If the difference curve is a single pick one, it means the block area has been through one JPEG compress, so this block belongs to B_i, and this area contains the insert image. If the difference curve is a double pick one, it means the block area has been through two JPEG compresses, so this block belong to B_o, and this area only contains the original image. So we can get the quality factor p_1 of the original image by analyzing the difference curve of the blocks that belong to B_o [9].

The process:

The algorithm was performed on a gray scale image. If it is a colored image then it was converted to grayscale. In certain cases, some preprocessing had to done. Here several gray scale images have been tried. One of the examples is shown below.

Distort the process:

The particular image shown below is saved as "the girl" into JPEG format with a quality factor of 25% (Fig.2 a)), then replace the eye portion in the image with surrounding pixels. JPEG image (with unknown quality factor) using Photoshop software, and finally save the image with a quality factor of 75% (Fig.2 b)).



a) Original Image **b) Tampered Image**

Fig 3: Tamper schematic

The process:

Step1 Divide the entire image into 8x8 or 16x16 blocks.

Step2 Perform JPEG compression with various quality factors p_i.

Step3 Plot difference curve and determine the quality factor of original image p_1.

Step4 Perform JPEG compression to the entire image for quality factor p_i.

Step5 Determine the threshold and mark the tampered area.

The same process can be carried out for color images also except that they need to be performed for each of R, G and B.

4. DETECTING CROPPED IMAGE

This section provides a solution to the situation where the tampered region of the image is cropped and then recompressed. In such situation, not only tamper detection but also the identification of; whether the image has undergone cropping must also be done. The figure below explains the scenario.

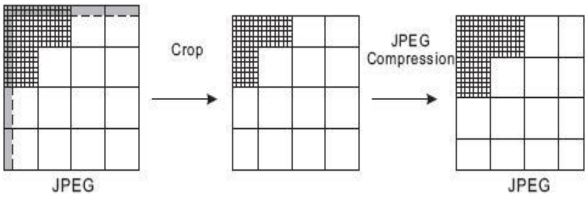


Fig 4: Cropped and Recompressed

The solution to this problem is to identify whether the image has been cropped and recompressed from another JPEG image. For that:

a. Detection of Blocking effects

b. Symmetricity from Blocking Artifacts

One of simple and effective ideas for detection of JPEG block artifacts have been proposed in [11]. In [11], it assumes that if there is no compression the pixel differences across blocks should be similar to those within blocks. The differences across blocks should be different due to block artifacts if the image is JPEG compressed. Then the difference within a block and spanning across the block can be determined.

Then histogram of this difference will be plotted after which the energy difference between both the histograms will be plotted. After plotting the energy difference curve, we will be able to see that the difference is larger across the JPEG boundary.

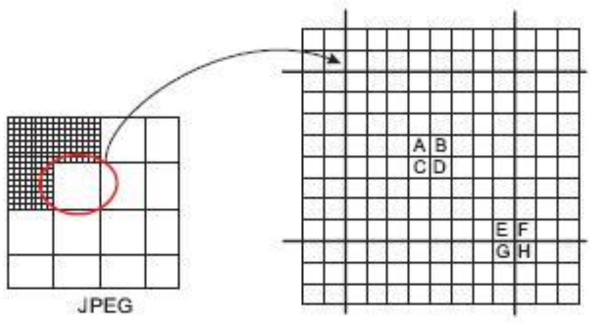


Fig 5: Blocking Artifact Detection

At first divide an image into non-overlapping 8 × 8 blocks. For each block, we compute **Z'(x, y)** and **Z''(x, y)** where **Z'(x,y)** and **Z''(x,y)** are the differences within the block and across the block respectively. Then the difference between the histograms **K(x, y)** is computed and get the average of **K(x,y)**, denoted as **M(x,y)**. The matrix **M(x, y)** is called the blocking artifact characteristics matrix (BACM) with which a contour map will be plotted. [12]

Based on the characteristics of BACM contour map, we will be able to identify whether the image is normal image, cropped image or uncompressed image.

5. CONCLUSION

While creating the digital forgery, a portion of the image will be copied and pasted in the same image or in different image in order to manipulate or hide the information of the target image. We have used a method that utilizes BACM properties in order to detect whether an image is cropped or not. To deal with SDJPEG problem, a block detection method which detects copy-paste tampering on an image has been combined with the above technique which provides an effective result.

6. ACKNOWLEDGEMENT

During the paper preparation, many reviewers provided many valuable constructive comments. I thank all.

7. REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukas, Detection of Copy-Move Forgery in Digital Images [J], Proceedings of Digital Forensic Research Workshop, 2003: 1-10.

[2] A.C. Popescu and H. Farid, Exposing digital forgeries by detecting traces of re-sampling, *IEEE Trans. on Signal Processing*, vol. 53, no. 2, pp. 758–767, 2005.

[3] A.C. Popescu and H. Farid, Exposing digital forgeries in color filter array interpolated images, *IEEE Trans. on Signal Processing*, vol. 53, no. 10, pp. 3948–3959, 2005.

[4] T.T. Ng, S.F. Chang, J. Hsu, L. Xie, and M.P. Tsui, Physics motivated features for distinguishing photographic images and computer graphics [J], Proc. of ACM Multimedia, Singapore, vol. 5, pp. 239.248, November 2005.

[5] J. Fridrich, M. Goljan, and R. Du, Steganalysis based on JPEG compatibility, in Proc. SPIE Multimedia Systems and Applications IV, Denver, CO, Aug. 2001, pp. 275–280.

[6] Z. Fan and R. L. de Queiroz, Identification of bitmap compression history: JPEG detection and quantize estimation, IEEE Trans. Image Process., vol. 12, no. 2, pp. 230–235, Feb. 2003.

[7] R. Neelamani, R. D. Queiroz, Z. Fang, and R. G. Baraniuk, JPEG compression history estimation for color images, IEEE Trans. Image Process. vol. 15, no. 6, pp. 1365–1379, Jun. 2006.

[8] Meng Xian-Zhe, Niu Shao-Zhang and Zou Jia-chea, Tamper Detection for Shifted double JPEG compression ,in Proc. Intelligent Information Hiding and Multimedia Signal processing, 2010 Sixth International Conference on 15-17 oct 2010.

[9] A.C. Popescu and H. Farid, Statistical tools for digital forensics [J], in Proc. of the 6th International Workshop on Information Hiding, Toronto, Canada, May 2004, vol. 3200 of LNCS, pp. 128–147

[10] Z. Fan and R.L. de Queiroz, Identification of bitmap compression history: JPEG detection and quantizer estimation, IEEE Trans. on Image Processing, vol. 12, no. 2, pp. 230–235, February 2003.

[11] W. Luo, Z. Qu, J. Huang, and G. Qiu, A novel method for detecting cropped and recompressed image block, in \Proc. ICASSP, Apr. 2007, vol. 2, pp. 217–220.