International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

Detection of Image Forgery was Created from Bitmap and JPEG Images using Quantization Table

Tran Dang Hien
University of Engineering and Eechnology,
VietNam National Univerity,
VietNam

Pham Van At
Department of Information Technology,
University of Transportation and Communications,
VietNam

***Abstract*— Image forgery was often created by copy and paste of images of different origins. Because the image is used can be obtained from many sources in various formats, so image forgery is very diverse and plentiful. In this paper we present a method to detect forged images are created from the JPEG images or from a Bitmap image and a JPEG image. The method is based on the properties of quantization step in the JPEG compression schema, allow detection of regions forgery inserted in a host image.**

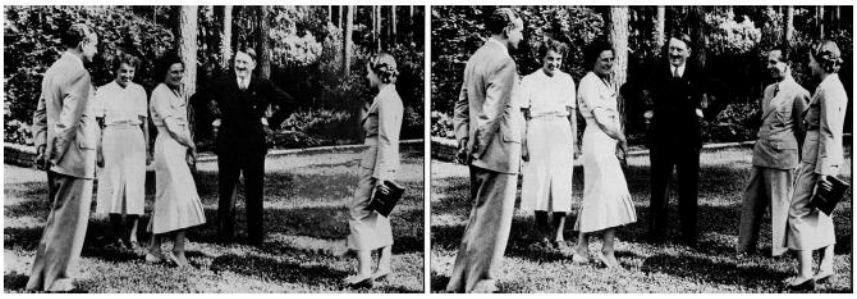
Keywords: Forensics, Image Forgeries, Image Tampering, JPEG compression, JPEG quantization, DCT.

I. INTRODUCTION

Image forgery very diverse and rich. There are many ways to create images forgery. Moreover, the image editing software are developed very powerful (such as Photoshop, GIMP) that a person does not need expert knowledge is also easy to create images forgery of their purpose. Here are some images forgery commonly in Fig. 1.

With the commonly of image forgery, now there is much research on methods of detecting image forgery, many new methods are given, as well as improve the efficiency of the method existed. Such as cloning, splicing, re-sampling, color filter array aberrations, sensor noise pattern, lighting inconsistencies [1] [2], reflection [12]. Although this technique is highly effective in most cases, but only appropriately applied to images with relatively high quality.

In this paper we propose a method based on the property of quantization in the JPEG compression process, the method does not depend on the characteristics of image quality and resolution. Recently, had a number of methods to detect image forgery based on JPEG compression format, as in [7] [8] proposed detection forgery method based on the irrational compression not entirely in the 8x8 blocks. In [3] [4] making method based on the periodic nature of the histogram of the image is JPEG double compression but on the actual application is very limited and difficult. In [9] develop methods to detect region forgery suffered double compression based on suport vector machine, this method needs a large image database for training. Our method was based on the properties information loss of quantization step in the JPEG compression schema, which is as advantages as effective methods existed and easily applied in practice. The next section of the paper are as follows: *2. Introduction Bitmap image and JPEG image, 3. Detecting images forgery based on the properties of quantization step, 4. Experience, and 5. Conclusion.*



In 1937. The image forgery (left), Joseph Goebbels was removed from the original image (right).

In 1939. The image forgery (left), King George VI was removed from the original image (right).

In 2010. The image forgery of president Kim Jong 2 with the army commanders.

In 2011. The image forgery of Iran's missile tests

Fig. 1. Example of Images forgery.

II. BITMAP IMAGE AND JPEG IMAGE

A. Bitmap image

Bitmap image format proposed by Microsoft, with extension BMP, this is kind of image transmission, widely used in computers and other electronic devices. Bitmap image is divided into three types: black and white image, grayscale images and color images.

Black and white image: images that each pixel is only one of two states, 0 and 1 to represent the state of black or white pixels.

Grayscale image: the image that each pixel is represented by a value and that the light intensity of the pixels.

Color image: each pixel is represented by three RGB values, the quantity for each R, G, B will be a corresponding color values. The colors of image up to 256^3. But some real color of an image can be quite small. To save memory, the image is less than 256 the number of colors, the colors of the pixels are stored as color palette. With the large number of colors, the image pixel color is not organized as the color palette, while the value of the pixel is the value of the color components R, G, B.

With a number of large color images, depending on image quality, which determines the number of bits to represent each color is usually 24 bits or 32 bits. With 24 bits image, each color component is represented by a byte (8 bits).

B. JPEG image

JPEG format is the result of collaboration between the International Telecommunications Union (ITU), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC). Its official name is "ISO / IEC 10918-1 Digital compression and coding of continuous-tone still images" or "ITU-T Recommendation T.81".

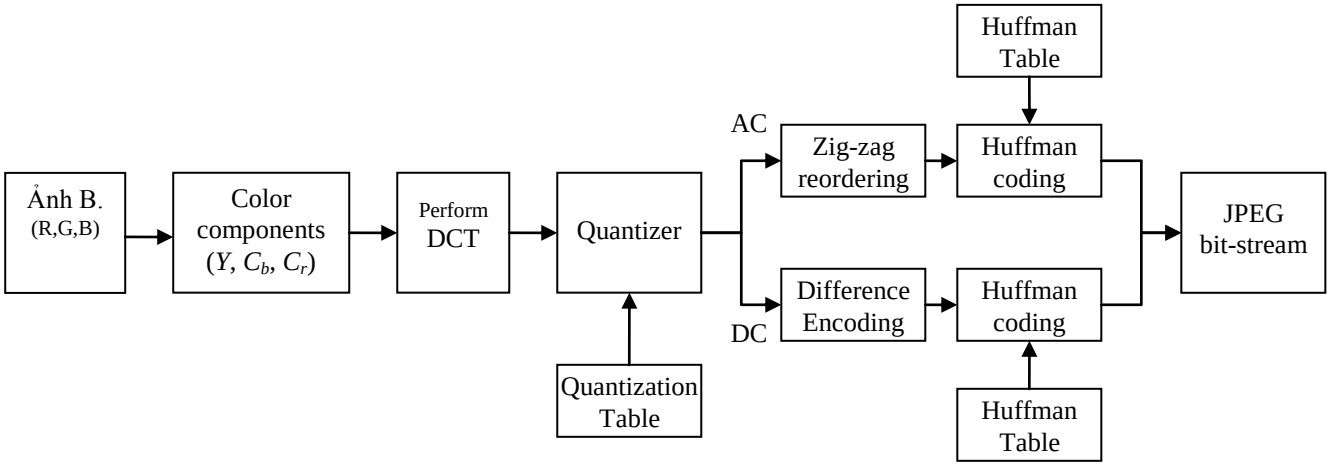


Fig. 2. JPEG compression process baseline

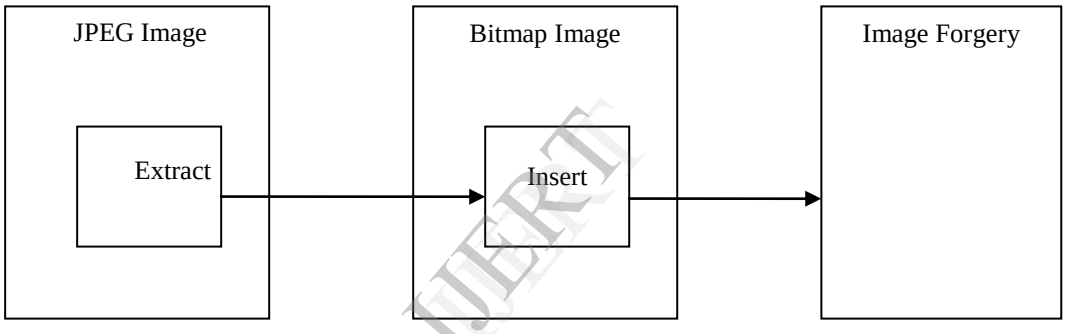


Fig. 3. The process of creating image forgery type 1

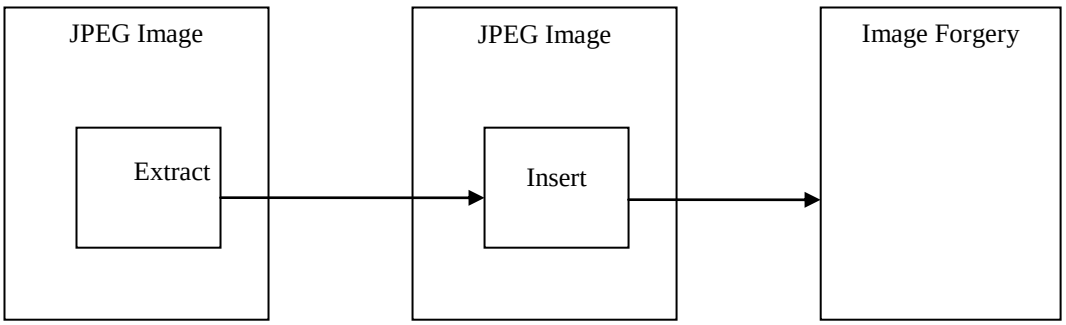


Fig. 4. The process of creating images forgery type 2

With JPEG compression scheme baseline JPEG, an RGB image is first converted to luminance space / chrominace (YCbCr). Each channel is then divided into 8 * 8 pixel blocks. These values continue to be converted from unsigned integer [0,255] to the integer [-128,127]. Following each block is converted to frequency space using 2-D Discrete Cosine Transform (DCT). Call each DCT coefficient is C, C continues to be quantized by q values:

$$\hat{C} = round(C / q)$$

Here quantized value q depends on the frequency and channel. The larger the value of q higher compression ratio and image quality after compression is lower. After several quantized DCT coefficients will become 0 (especially for high-frequency region). Finally, these coefficients are compressed using Huffman method and Runlengh. JPEG compression process as described in the following diagram in Fig. 2. Similarly, to extract JPEG images taken steps backwards with JPEG compression process as above.

III. DETECTING IMAGE FORGERY BASED ON THE PROPERTIES OF QUANTIZATION STEP

The following, the paper presents method to detect image forgery:

A. *Image forgery*

Type 1: Bitmap image is forged. Regions forgery were inserted, which were taken from JPEG images (Fig. 3).

Type 2: JPEG image is forged. Regions forgery were inserted, which were taken from JPEG images, has compression quality other (Fig. 4).

Comment:

- The region is inserted can be extracted from JPEG images.

- The JPEG image quality similar or different.

B. *Theoretical foundations*

The method is based on the properties of quantization step, in the following lemma:

Lemma: Suppose the discrete cosine transform is performed exactly in the JPEG compression scheme (Figure 1), a JPEG image is double compressed with the same compression ratio, the value of R, G, B at each pixel does not change (image do not change).

Prove the lemma:

Some notation:

Bitmap original is B.

JPEG image obtained after compression B (first compression) is J1.

Bitmap images obtained after decompression J1 is B1.

JPEG image obtained after compression B1 (second compression) is J2.

Bitmap images obtained after decompression J2 is B2.

So, the lemma need to prove two bitmap images B1 and B2 are equal (the value of R, G, B are equal).

The notation in the process of quantization and inverse quantization of the first and second compression is described as in the diagram below:

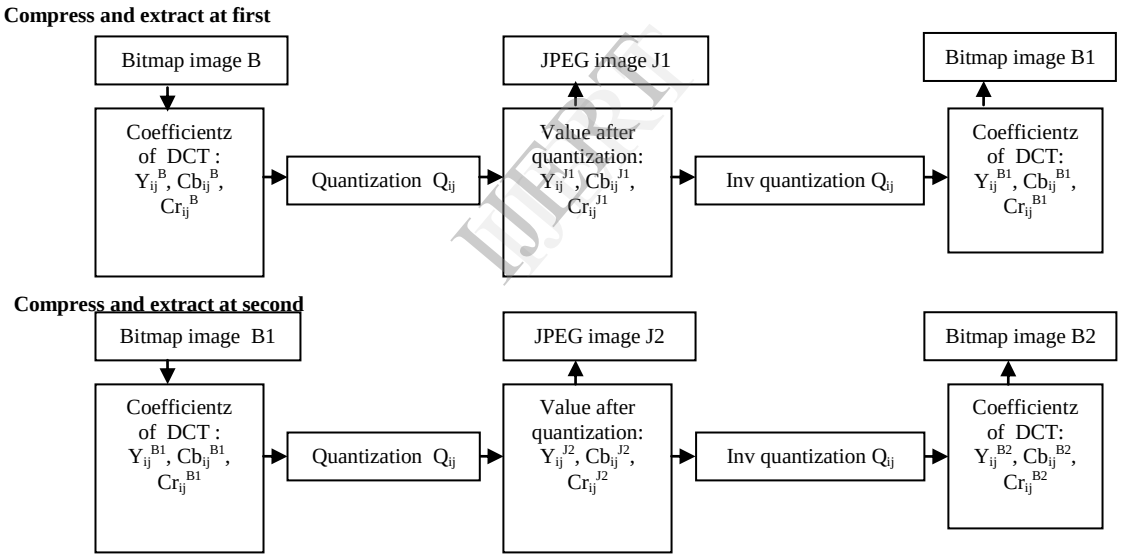


Fig. 5. Compress and exact Bitmap image B, B1

Considering the value of the component Y, in the quantization step, Y_{ij}^{J1} is calculated as follows:

$$Y_{ij}^{J1}=round(Y_{ij}^{B}/Q_{ij})$$

Perform decompression JPEG image J1 obtained bitmap image B1, in inverse quantization step Y_{ij}^{B1} is calculated as follows:

$$Y_{ij}^{B1}=Y_{ij}^{J1}*Q_{ij}$$

Perform a second compression from bitmap image B1 obtained JPEG image J2, value Y_{ij}^{J2} by :

$$Y_{ij}^{J2}=round(Y_{ij}^{B1}/Q_{ij})$$

It follows:

$$Y_{ij}^{J2}=round(Y_{ij}^{J1}*Q_{ij}/Q_{ij})=Y_{ij}^{J1}$$

Perform decompression JPEG image J2 obtained bitmap image B2, in inverse quantization step Y_{ij}^{B2} is calculated as follows:

$$Y_{ij}^{B2}=Y_{ij}^{J2}*Q_{ij}$$

Because $Y_{ij}^{J2}= Y_{ij}^{J1}$ so:

$$Y_{ij}^{B2}=Y_{ij}^{J1}*Q_{ij}= Y_{ij}^{B1}$$

Similar to the Cb and Cr components, so:

$$Cb_{ij}^{B1}=Cb_{ij}^{B2} \text{ và } Cr_{ij}^{B1}=Cr_{ij}^{B2}$$

Because, suppose the discrete cosine transformation is performed exactly in the JPEG compression scheme, so the value of R, G, B of Bitmap image B1 and B2 are equal. Thus the lemma is proven!

In the process of quantization step has differences, so it follows properties:

Properties 1: *A double compressed JPEG with different compression ratio, the image will be changed.*

Properties 2: *A bitmap image is compressed with JPEG compression schema will also be changed.*

C. Algorithm for detecting forgery images

The algorithm is based on the lemma and the properties in section III.B, the algorithm uses the quantization table Q_α (α=1,…,100), and a value d $\in$ {1,2,…,10} as the threshold to determine the forgery (discrete cosine transform with the inaccuracy). The method is implemented as follows:

Input: Image F , size mxn

(F could be the image original or image forgery type 1 or 2).

Output: region forgery of image were inserted.

Step 1. Selected α=1

Step 2. $Q=Q_\alpha$

Step 3. Image compression with quantization table Q received F'.

Step 4. Determine the subtract of the two image:

$$G=F \Theta F'$$

$$G_{ij}(R)=|F_{ij}(R) - F'_{ij}(R)|$$

$$G_{ij}(G)=|F_{ij}(G)-F'_{ij}(G)|$$

$$G_{ij}(B)=|F_{ij}(B)-F'_{ij}(B)|$$

Step 5. Selected d, determine union:

$$Wd=\{(i,j)|G_{ij}(R)+G_{ij}(G)+G_{ij}(B)\leq d\}$$

- If Wd is exist then Wd is the region forgery (the Wd correspond to the inter-domain and sizes greater threshold value) => end of the algorithm.

- Case else switch to step 6.

Step 6: $\alpha=\alpha+1$

- If $\alpha\geq 100$, Image is original => end of the algorithm.

- If $\alpha<100$, goto step 2.

The correctness of the algorithm: Suppose the image *F* has at least one region *W* with compression quantization table Q_0 be inserted. According to the lemma and the properties when the algorithm is run with $Q = Q_0$ then obtained *Wd* equivalent approximately W accord threshold d.

IV. EXPERIENCE

We have programmed algorithm and use photo editing software Photoshop to create some image forgery, also use this software to compress JPEG images forgery with different compression ratio. Then proceed to subtract the pixel values of the image is compressed JPEG with image forged obtained a pixel matrix, show the matrix pixel is obtained. With the same compression rate, some area will appear black, which is the forgery region. Here is an illustrative example, images forgery are created from JPEG images as follows in Fig. 6.

Test results of the algorithm with the image forgery at compression various ratios, subtraction of image forgery with compressed images at various ratios to show up in the form of multi-level gray, at compression ratio 40 medium, the region fogery almost entirely black, as shown below in Fig. 7.

Fig. 6. Images forgery are created from JPEG images

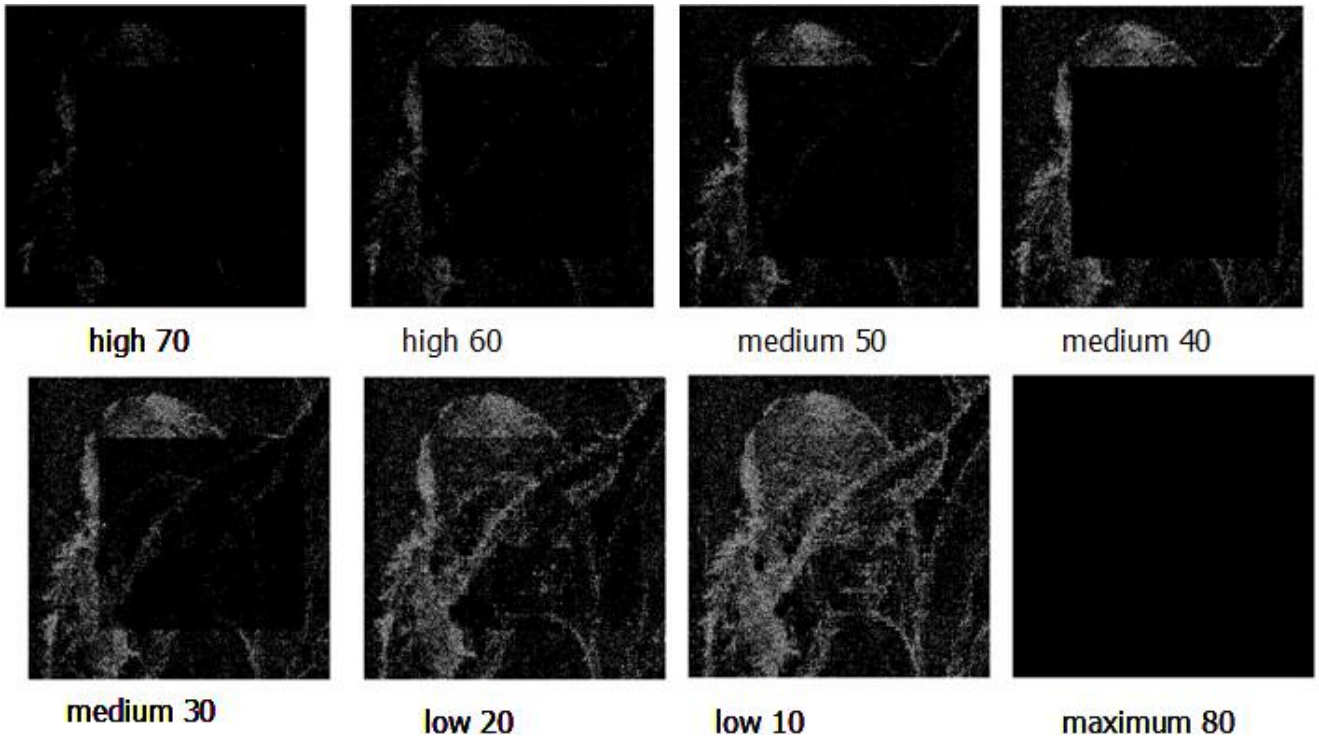


Fig. 7. Results of the algorithm with the image forgery at compression various ratios

V. CONCLUSION

With the development of the Internet has helped the process of distribution and dissemination of images becomes easy and fast. In recent years, image forgery has affected science, law, politics, the media and business. A number of cases have created a national and international events. Therefore, detecting images forgery becomes increasingly urgent and difficult.

Based on the research process of JPEG compression and properties of quantization step. We present a method to detect images forgery. The method does not depend on the characteristics of image quality and resolution of the image. To apply the method in practice, also need to build the library of quantization tables from photo editing software, cameras, etc... to determine whether the image is compressed by devices or the application software corresponds to the quantization process.

REFERENCES

[1] H. Farid (2011), *"Digital image forensics"*, Lecture Notes, Darmouth college, 2011.

[2] H. Farid (2009), "A survey of image forgery detection", *IEEE Signal Processing Magazine*, vol. 2, no. 26, pp. 16–25.

[3] A.C. Popescu (2005), "Statistical tools for digital forensics", Phd Thesis, Darmouth College.

[4] B. Mahdian and S. Saic (2009), "Detecting double compressed JPEG images", In *International Conference on Imaging for Crime Detection and Prevention*.

[5] J. Fridrich (2009). "Digital image forensic using sensor noise". *IEEE Signal Processing Magazine*, 26(2):26-37.

[6] J. Fridrich, D. Soukal, and J. Lukas (2003), "Detection of copy-move forgery in digital images," in Proceedings of Digital Forensic Research Workshop.

[7] S. Ye, Q. Sun, and E. Chang (2007), "Detecting digital image forgeries by measuring inconsistencies of blocking artifact," *in 2007 IEEE International Conference on Multimedia and Expo*, pp. 12–15.

[8] W. Luo, Z. Qu, J. Huang, and G. Qiu (2007), "A novel method for detecting cropped and recompressed image block," *in IEEE Conference on Acoustics, Speech and Signal Processing*, pp. 217–220.

[9] J. He, Z. Lin, L. Wang, and X. Tang (2006), "Detecting doctored JPEG images via DCT coefficient analysis," in *European Conference on Computer Vision*, Graz, Austria.

[10] ISO/IEC JTC1 (1991), "Digital compression and coding of continuous-tone still images, Part 1: Requirements and guidelines," Draft International Standard 10918-1.

[11] G. Wallace (1991), "The JPEG still picture compression standard," *IEEE Transactions on Consumer Electronics*, vol. 34, no. 4, pp. 30–44.

[12] J. O'Brien and H. Farid (2012 in press), "Exposing Photo Manipulation with Inconsistent Reflections", *ACM Transactions on Graphics*.