Spring 5-31-2011

Digital image forensics

Fei Long
New Jersey Institute of Technology

Copyright Warning & Restrictions

The copyright law of the United States (Title 17, United States Code) governs the making of photocopies or other reproductions of copyrighted material.

Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be "used for any purpose other than private study, scholarship, or research." If a, user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of "fair use" that user may be liable for copyright infringement,

This institution reserves the right to refuse to accept a copying order if, in its judgment, fulfillment of the order would involve violation of copyright law.

Please Note: The author retains the copyright while the New Jersey Institute of Technology reserves the right to distribute this thesis or dissertation

Printing note: If you do not wish to print this page, then select "Pages from: first page # to: last page #" on the print dialog screen

ABSTRACT

DIGITAL IMAGE FORENSICS

by

Fei Long

Digital image forensics is a relatively new research field that aims to expose the origin and composition of, and the history of processing applied to digital images. Hence, the digital image forensics is expected to be of significant importance to our modern society in which the digital media are getting more and more popular. In this thesis, image tampering detection and classification of double JPEG compression are the two major subjects studied. Since any manipulation applied to digital images changes image statistics, identifying statistical artifacts becomes critically important in image forensics. In this thesis, a few typical forensic techniques have been studied. Finally, it is foreseen that the investigations on endless confliction between forensics and anti-forensics are to deepen our understanding on image statistics and advance civilization of our society.

DIGITAL IMAGE FORENSICS

by
Fei Long

A Thesis
Submitted to the Faculty of
New Jersey Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Electrical Engineering

Department of Electrical and Computer Engineering

May 2011

APPROVAL PAGE

DIGITAL IMAGE FORENSICS

Fei Long

Dr. Yun Q. Shi, Thesis Advisor — Date
Professor of Electrical and Computer Engineering, NJIT

Dr. Ali N. Akansu, Committee Member — Date
Professor of Electrical and Computer Engineering, NJIT

Dr. Richard A. Haddad, Committee Member — Date
Professor of Electrical and Computer Engineering, NJIT

BIOGRAPHICAL SKETCH

Author: Fei Long

Degree: Master of Science

Date: May 2011

Undergraduate and Graduate Education:

- Master of Science in Electrical Engineering,

  New Jersey Institute of Technology, Newark, NJ, 2011

- Bachelor of Science in Information Engineering,

  The Chinese University of Hong Kong, Satin, Hong Kong, 2008

Major: Electrical Engineering

ACKNOWLEDGMENT

First and foremost, I would like to show my deepest gratitude to my supervisor, Dr. Yun-Qing Shi, a respectable and responsible scholar, who has provided me with valuable guidance during my graduate study. Without his enlightening instruction, kindness and patience, I could not have completed my thesis.

I shall extend my thanks to all my professors at New Jersey Institute of Technology, especially Dr. Ali Akansu, Dr. Durga Misra and Dr. Richard Haddad for the great help for my graduate study and life. My sincere appreciation also goes to all of my friends. In particular, I would like to thank: my MS thesis committee members: Yun-Qing Shi, Ali Akansu and Richard Haddad; My colleagues from the Intelligent Multimedia Laboratory: Patchara Sutthiwan, Hai-Feng Xiao, Guan-Shuo Xu, Jing-Yu Ye and Peng Meng. Finally, but not the least, my family and my girlfriend.

TABLE OF CONTENTS

TABLE OF CONTENTS

Chapter **Page**

CHAPTER 1

INTRODUCTION

1.1 Seeing Is Believing ?

On October 14 of 2008, Doug Beaver, the software engineer of Facebook which is one of the most popular social networking service and websites in the world, announced that there are over 10 billion photos hosted by Facebook. As can be imagined, the expanding potential of images not only makes images one of the most widely-used ways to convey information, but also bring about many popular multimedia editing software like Adobe Photoshop and Corel Painter that are capable to modify images in a relatively simple way. Editing images are no longer experts' franchise since common people are also able to make good quality tampering or forgeries. Therefore the authenticity of digital images may be a questionable in some cases.

Images are always utilized by media such as TV or newspaper to convey information. In addition, they also act as the evidence of what has been reported to the public. But the ease of image forgery with high quality resulted in the suspicion of the authenticity and integrity of an image published by media. In 2003, Brian Walski, an L.A. Times photographer at that time, was fired due to the fact that he composed a superior picture by combining two of his pictures together [1], which is shown in Figure 1.1. While Brian was in Iraq, he captured several pictures of a British soldier speaking to Iraqi civilians. Then he selected two pictures from them that have the best

quality and combined them together into a composite image, which finally resulted in the scandal and made him fired. In 2004, while Senator John Kerry was running for president, a scandal along with an old picture (shown as Figure 1.2) was shown to the public, in order to make him fail during presidential campaign. In the picture, John Kerry shared a podium with actress/anti-war activist Jane Fonda at an anti-war rally. But later it was proved to be a hoax, which was nothing but a composite picture. In 2006, Adnan Hajj, a former photographer of Reuters, admitted that he forged several pictures before publishing. From Figure 1.3, some clue may be found to the digital manipulation, where the dust seems like a composite that has been through clone manipulation. From the above examples as well as many other well-known forged images, people should no longer just simply take what TV or newspaper has reported as true. It is because that images, which always act as the evidence of the authenticity of the news reported, turn out to be undetectable by human eyes after being tampered. Therefore, the importance of authenticity of a picture, especially for those published to the public by media, leads to the increasing demand for more effective digital image forensics techniques. People believe that even if it is impossible to discriminate between forged images and natural images by human eyes, there are still some traces of digitally manipulation left.

(a)

(b) **(c)**

Figure 1.1 The composite image (a) of a British soldier speaking to Iraqi civilians was made by editing two natural images (b) and (c). [1]

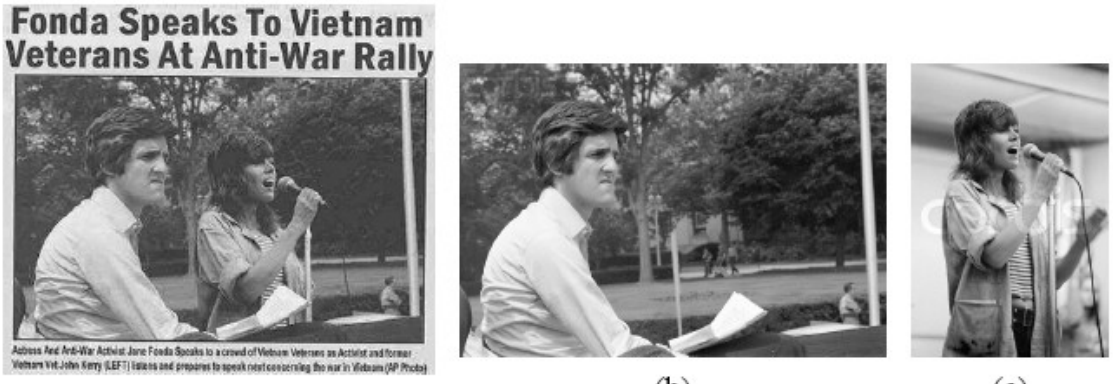


Figure 1.2 The well-known altered image of John Kerry and Jane Fonda (a) which was formed by two authentic images (b) and (c). [2]

From the above discussion, “seeing is believing” is no longer be that suitable for this society, which is getting increasingly getting digitized. Digital image forensics is

a relatively new research field that aims to expose the origin and composition of, and the history of processing applied to digital images. The main idea of image forensics is based on the fact that even if image forgeries can no longer be perceived by human eyes, statistical artifacts can still be exposed, indicating whether an image is tampered or not. To get a better understand of digital image forensics, it may be compared with two related fields of multimedia security, which are digital watermarking and steganography [3].

(a) **(b)**

Figure 1.3 Shown are (a) the original image captured by Adnan Hajj; (b) the forged image of (a). [4]

1.2 Digital Image Forensics, Digital Watermarking and Steganography

Generally speaking, recall that digital image forensics is a relatively new research field as well as a passive way that aims to expose the origin and composition of, and the history of processing applied to digital images. In contrast, digital watermarking is an active way that can be used to protect the authenticity of an image based on the information embedded in the carrier. On the other hand, steganography aims to secretly communicate via certain media, such as hiding some secret information to an

image, which is also an active process.

Digital watermarking technique is the process of embedding information into a digital signal in a way that is difficult to remove [5]. Although information or extra bits are added to the original carrier such as image, they do not significantly influence the functions and properties of the carrier and also it is almost undetectable using human eyes. Based on the embedded information, it is possible to achieve various functions such as identifying the image source, purchaser identification, sending confidential messages or judging whether the carrier has been tampered or not.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message [6]. To the contrary, the aim of steganaysis is to detect whether hidden information is involved via steganography in an image. To some extent, steganography is similar to image tampering since it also changes the original image, though the goal of such “tampering” is for confidential communication rather than for others. Therefore for both image tampering and steganography, statistical correlations are modified. Therefore there may be some detection methods that are applicable to both tampering detection and steganalysis, especially for those mathematical and computational algorithms that examine statistical correlations. As to be discussed in Section 2.2.1, some frameworks that are suitable for both image forensics and steganalysis have been reported [2], [7], [8], [9], [10].

As a passive way, digital image forensics may not have the prior knowledge of the tampered image. In practical use, it is impossible to get prior knowledge for most of

the cases, which makes digital image forensics remarkably important even compared to digital watermarking or steganography.

CHAPTER 2

TAMPERING DETECTION

Powerful multimedia editing tools such as Adobe Photoshop and Corel Painter make image tampering much easier to carry out than before. They are widely used in the whole world. Besides those experts in image editing, modern software also make it convenient and easy for common people to forge images with good quality. Image tampering techniques are widely used in our normal life such as picture beautification. On the other hand, they are also used as powerful tools for political or even racial issues, which make detection of doctored images important.

The description within this section mainly focuses on image tampering detection and some related fields. Firstly, several existing and widely-used image tampering techniques are introduced. For example, object removal denotes directly removing an object from an image. Cut-and-paste denotes copying a part of an image to another. Afterwards, some tampering detection techniques are shown in detail such as machine learning or wavelet domain based techniques.

Alhough some different methods have been proposed, most of the techniques are based on statistical artifacts which examine statistical correlations. If an image has been tampered, the statistical correlations among neighboring pixels and among DCT coefficients are modified. Therefore most of the recent research is to explore the ways to expose the statistical artifacts. As can be imagined, some signal processing tools are being widely used due to their statistical nature. For example, discrete wavelet

transform not only decorrelates signals but also introduces the interdependencies across and within scales. Hidden Markov models along with its three main topics (Forward, Viterbi and Baum-Welch algorithms) evaluate hidden states based on observed data. Markov based transition probability matrix monitors the statistical properties among neighboring pixels or among DCT coefficients in a global way, and so forth.

2.1 Introduction to Basic Tampering Methods

When using multimedia editing software such as Adobe Photoshop, generally speaking, basic tampering methods can be divided into three classes. The first one is to remove a certain part from an image, which is known as object removal manipulation. It is obvious that this manipulation has little relationship with other images but itself. The second one is to copy an object from another or the same image to an image. The third one is kind of a CG based technique that maybe used to form a certain object using computer program or add some extra effect to make the forged image appears to be as natural as possible.

2.1.1 Object Removal

The first class to be introduced here is object removal. Compared to the other two classes, it appears to be more straight-forward and direct. If people hope to use Adobe Photoshop to realize object removal manipulation, it’s nothing but to firstly use lasso tool or pen tool to form a region that needs to be removed, and then simply delete the highlighted region from the current layer. As can be seen, until now, what to be

emphasized is only one image rather than multiple images.

After removing a certain object, in order to make it natural, the forger needs to deal with the removal region by using some certain techniques. The simplest case is to directly copy a region of the same image and then paste it to the removed region. As can be seen from Figure 2.1, firstly the hand is removed from the image and then to copy and paste the neighboring area to the removed region to make the forged image seems real. In case of the obvious border or other traces that may imply the manipulation of object removal, some resampling methods are used such as rotation, re-sizing or portion stretching.

Figure 2.1 An example of object removal. [11]

Besides, a well-known technique called in-painting [12] is being widely used. In-painting is the process of reconstructing lost or deteriorated parts of images and videos. It reconstructs the missing area by considering those pixel values or areas around it. In this way, it is illustrated that statistical correlations between neighboring areas and pixels are to be considered. Then from the boundary to the center of the

missing area, in-painting technique predicts the pixel value iteratively.

2.1.2 Splicing

Besides removing a certain object, covering an area with a new object is another way of image tampering, which is also known as splicing or cut-and-paste method. Similarly to previous section, if Adobe Photoshop is to be used to achieve this function, the highlighted region can be easily selected and then use it to cover a region of another image. Again, in order to smooth the boundaries and reduce the obvious inconsistencies between neighboring areas, resampling techniques are to be used, such as re-sizing, rotation and portion stretching. In Figure 1.2, the well-known tampered image of John Kerry and Jane Fonda, which underwent splicing manipulation, is shown.

2.1.3 Computer Graphics (CG) based Techniques for Tampering

Besides previous methods, by using the powerful editing software such as Adobe Photoshop, common people are also able to use CG based techniques to forge a certain picture. Believe it or not, many 2D designers are able to use those editing software to draw an image that looks as if it were a photographic picture. From Figure 2.2, how a real and natural image can be drawn using Photoshop is shown. If just judged by our human eyes, it is almost impossible to tell whether it is captured by a digital camera or drawn using software.

Figure 2.2 Mouse drawing results using Photoshop. [13]

2.2 Some Tampering Detection Methods

In this section some of the recent tampering detection techniques are presented in details based on some well known previous work such as [14], [15], [16] that emphasize on cloning or splicing manipulation detection.

2.2.1 Moments and Markov based Splicing Detection Technique

As described in 2.1.2, splicing is widely used by common people and even experts to forge an image. Thus splicing detection is of great importance and also attracts many researchers' attention. Image splicing is a simple process that crops and pastes areas from an image to another or even the same image without post-processing as smoothing. The simplicity and directness of splicing seem to be the main reason why it is one of the most widely used scheme in the field of image tampering.

Based on the contributions of previous research like [17] and [18], Shi et al. [4] developed a method based on multi-sized block discrete cosine transform (MBDCT),

moments of characteristic functions as well as wavelet sub-bands, and Markov transition probability matrix. By using these features, considerable accuracy rate is obtained.

The main flowchart of this technique is shown as Figure 2.3.

As to be discussed in Chapter 3, block discrete cosine transform (BDCT) is being widely used in various fields like multimedia compression such as JPEG due to the following two properties. The first one is the ability of signal decorrelation. The second one is energy compaction, which denotes the fact that most of the energy locates close to the DC mode at the left top of a block.

Although in spatial domain, it is impossible for human eyes to perceive the changes after splicing manipulation. In frequency domain or to say DCT domain, the coefficients indeed reflect the changes caused by splicing. Since single-sized block DCT is not enough to capture those changes, Multi-sized block DCT (MBDCT) is used to generate the features for classification. Then for each result calculated in previous step, the features are extracted based on statistical moments and Markov transition probability.

To generate moment based features, characteristic functions of both 1-D and 2-D cases are calculated as an intermediate process. The flow chart of moment feature generation is shown as Figure 2.4(a).

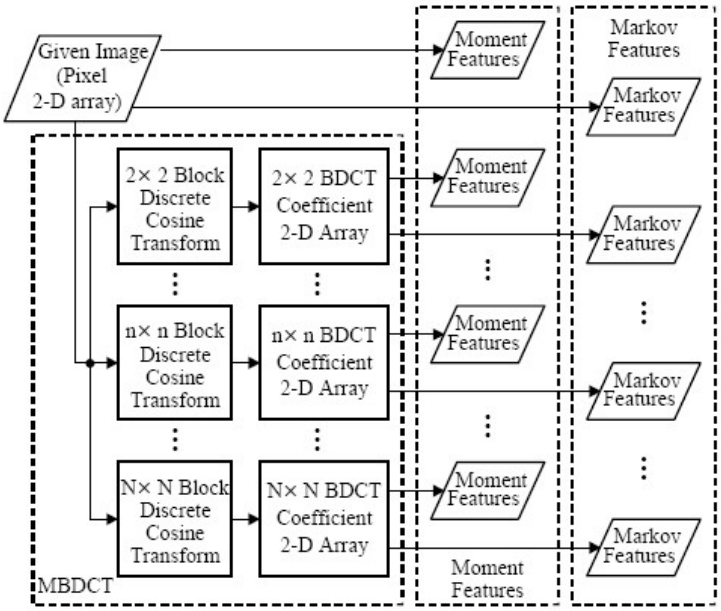


Figure 2.3 Flowchart for feature extraction. [4]

The prediction error array is utilized to strengthen the statistical properties brought about by splicing manipulation. Consider a pixel with value x and the neighboring pixels are described as Figure 2.4(b), the values of prediction 2-D array can be obtained by:

$$\Delta x = x - \bar{x} = x - sign(x) \cdot \{|a| + |b| - |c|\} \tag{2.1}$$

$\bar{x}$ denotes the prediction value and x denotes the exact value of the pixel. Then for 1-D moment features, firstly discrete wavelet transform (DWT) is taken to both DCT 2-D coefficients array and prediction-error 2-D array. Then histograms of low-low sub-bands are generated respectively. Please refer to Appendix A for more details about DWT. Finally 1-D moment features are calculated according to:

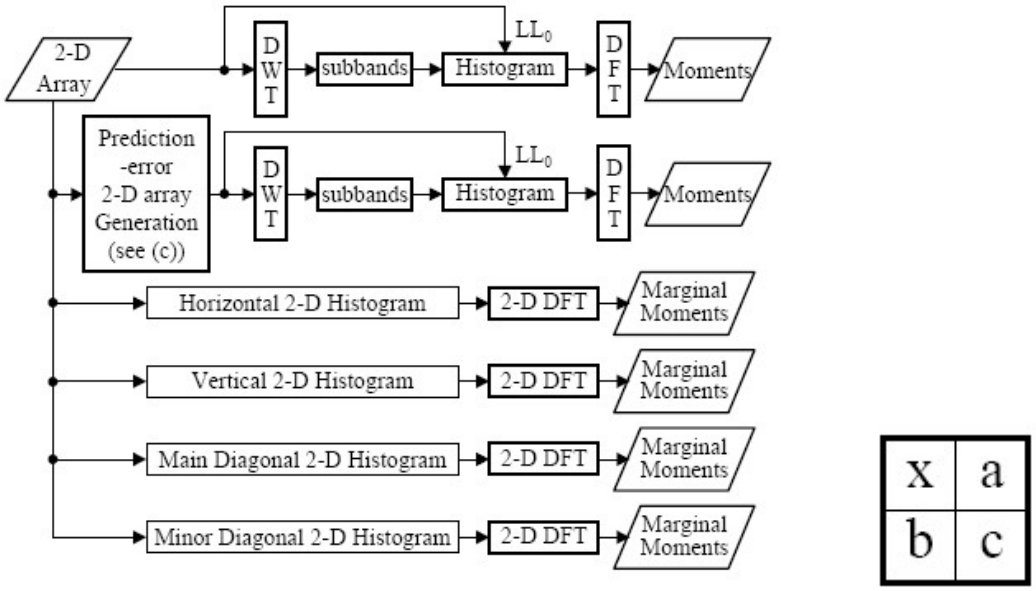


Figure 2.4 Shown are: (a) Main flowchart for moment based feature extraction; (b) prediction context. [4]

$$M_l = \frac{\sum_{i=1}^{K/2} x_i^l \, |H(x_i)|}{\sum_{i=1}^{K/2} |H(x_i)|} \tag{2.2}$$

Here l represents the order of moment. For 2-D marginal moment features, the histograms regarding those four different directions can be calculated by using the following formula, which is just the 2-D case of (2.2):

$$M_l = \frac{\sum_{i=1}^{K/2} x_i^l \, |H(x_i)|}{\sum_{i=1}^{K/2} |H(x_i)|} \tag{2.3}$$

Here $H(u_i, v_i)$ stands for the characteristic component at frequency (u_i, v_i) .

Besides moment based features introduced above, the other group of features used in this technique is Markov transition probability based features, which also has the capability to reflect the changes of statistical correlations. Similarly to the prediction-error 2-D array for moment based features extraction, four kinds of difference 2-D arrays are calculated for Markov based features, which are defined as:

$$F_h(u,v) = F(u,v) - F(u+1,v) \tag{2.4}$$

$$F_v(u,v) = F(u,v) - F(u,v+1) \tag{2.5}$$

$$F_d(u,v) = F(u,v) - F(u+1,v+1) \tag{2.6}$$

$$F_m(u,v) = F(u+1,v) - F(u,v+1) \tag{2.7}$$

Those 2-D arrays reflect the statistical properties in terms of two neighboring pixels or BDCT coefficients along horizontal, vertical, main diagonal and minor diagonal directions. Here *F(u,v)* denotes either the pixel value of original image or absolute value of rounded BDCT coefficient. Then according to the main flow of Markov transition probability based features extraction shown in Figure 2.5, a threshold value T is introduced to reduce the computational complexity. That is to say, for each element in the difference 2-D array, if the value is larger than T or smaller than T, then it will be assigned to T or –T respectively. Then based on the results obtained as well as Bayes rule, transition probabilities matrices are derived according to the four formulae shown below that correspond to four directions respectively:

$$p\{F_h(u+1,v)=n \mid F_h(u,v)=m\}=\frac{\sum_v\sum_u \delta(F_h(u,v)=m, F_h(u+1,v)=n)}{\sum_v\sum_u \delta(F_h(u,v)=m)} \tag{2.8}$$

$$p\{F_v(u,v+1)=n \mid F_v(u,v)=m\}=\frac{\sum_v\sum_u \delta(F_v(u,v)=m, F_v(u,v+1)=n)}{\sum_v\sum_u \delta(F_v(u,v)=m)} \tag{2.9}$$

$$p\{F_d(u+1,v+1)=n \mid F_d(u,v)=m\}=\frac{\sum_v\sum_u \delta(F_d(u,v)=m, F_d(u+1,v+1)=n)}{\sum_v\sum_u \delta(F_d(u,v)=m)} \tag{2.10}$$

$$p\{F_m(u,v+1)=n \mid F_m(u+1,v)=m\}=\frac{\sum_v\sum_u \delta(F_m(u+1,v)=m, F_m(u,v+1)=n)}{\sum_v\sum_u \delta(F_m(u+1,v)=m)} \tag{2.11}$$

Again, for no matter statistical moment based features or Markov transition probability based features, they are derived according to both the image pixel 2-D arrays and the MBDCT coefficient 2-D arrays. During experiments, Support Vector Machine and Radial Basis Function kernel are used as classifier.

In this scheme, the choice of threshold T is one of the issues to be focused on. T is used to reduce the dimensionality of Markov features. To choose an appropriate value of T, following points are to be focused. Large T leads to remarkably computational complexity since the dimensionality of the transition probability matrix is too large. On the other hand, small T also results in inaccurate classification since it reduces the sensitivity of capturing the splicing artifacts. Table 2.1 shows the accuracy corresponding to different threshold T values. Since for T larger than 4, the

dimensionality turns out to be too large to manage, Table 2.1 evaluates the result with T equals to 2, 3 and 4 respectively. When T is larger than 2, most of the statistical artifacts can be captured by transition probability matrix, which is illustrated in [7] and also shown in Table 2.2. Therefore 3 appears to be the appropriate value for threshold T, since it not only makes the transition probability matrix consider most of the statistical artifacts brought by splicing, but also keep the dimensionality at an acceptable amount.

Table 2.1 Performance Comparison with Different Threshold T Values [7]

Feature sets	50-D features (T=2)	98-D features (T=3)	162-D features (T=4)
TN rate	87.58% (2.74%)	86.61% (3.00%)	87.61% (2.72%)
TP rate	79.70% (2.62%)	90.03% (2.63%)	90.69% (2.75%)
Accuracy	83.68% (2.06%)	88.31% (1.85%)	89.14% (1.50%)

TN and TP denote True Negative and True Positive.

Table 2.2 Mean and Standard Deviation of Percentage Numbers of Elements of Horizontal Difference JPEG 2-D Arrays Falling Within [-T, T] [4]

	[-1, 1]	[-2, 2]	[-3, 3]	[-4, 4] (*)	[-5, 5]	[-6, 6]	[-7, 7]
Mean	84.72	88.58	90.66	91.99	92.92	93.60	94.12
Standard deviation	5.657	4.243	3.464	2.836	2.421	2.104	1.850

The outstanding accuracy rate (more than 90%) shows the effectiveness and potential of such moment and Markov transition probability based method. Due to the fact that it focuses on the statistical artifacts caused by splicing manipulation, such technique not only yields a considerable performance rate, but also has the potential to be extended to other related fields such as steganalysis. As mentioned in Section 1.2, for both image tampering and steganography, the statistical correlations are

changed. Although the training data and objective are different from each other, by taking this Markov and moment based technique, not only discrimination between natural images and tampered images can be achieved, but also for natural images and stego images.

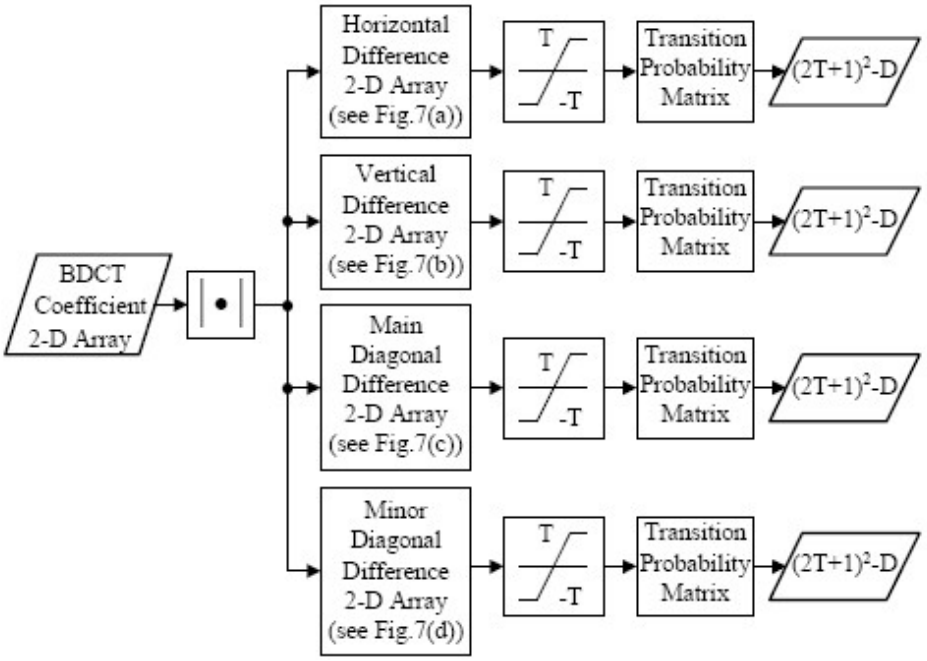


Figure 2.5 Main flow charts for Markov based feature extraction. [4]

2.2.2 Detection of Resampling Traces for Tampering Detection

As mentioned in 2.1, some tampering or post-processing methods including rotation, re-sizing or portion stretching require resampling the original image. Resampling is often hardly perceptible by human eyes, but it actually brings about some specific correlations which can be detected as the evidence for image tampering. Popescu [19] developed an algorithm aiming at detecting resampling manipulations which is to be introduced in this section. Note that in matrix form, resampling process can be described as:

$$y = Ax \tag{2.12}$$

Here vector x and y denote the original signal and resampled signal respectively. Matrix A contains all the information for resampling process.

To illustrate resampling, let's consider a simple example first. If factor 4/3 is taken as the resampling factor, then it means that for the original signal, every three samples are resampled by four samples. Based on linear interpolation, it is obvious that for the first sample in the resampled signal, say y, it is the same as the sample of the original signal, denoted as x. But for the second sample of y, it is actually between the first and the second sample of x, which locates at 0.75. Therefore the second sample of y can be presented as a linear combination of the first and the second sample of x in which the weights correspond to the distance between those two samples of x as well and the second sample of y respectively. Furthermore, since 0.75, the exact location of the second sample of y if mapping to the original signal lattice, is closer to the second sample of x than to first sample of x. Just based on the proportion of the two distances, the value of the second sample of y can be assigned by: $0.25x_1 + 0.75x_2$. In this way matrix A can be formed as:

$$A_{4/3} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0.25 & 0.75 & 0 & 0 \\ 0 & 0.50 & 0.50 & 0 \\ 0 & 0 & 0.75 & 0.25 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{2.13}$$

Note that due to the periodicity of the correlations, the above matrix is just within a single period. By linear algebra, during a single period, each sample within vector y, can be represented by linear combination of some neighboring samples. For example, in the previous example with resampling factor equals to 4/3, the following relationship between y_3 and some of its neighbors can be found as:

$$y_3 = (-1/6)y_1 + (2/3)y_2 + (2/3)y_4 - (1/6)y_5 \tag{2.14}$$

which implies that for arbitrary resampling factor p/q, each sample of resampled signal y may equal to a certain linear combination of its 2N neighbors, denoted as:

$$y_i = \sum_{k=-N}^{N} \alpha_k y_{i+k} \tag{2.15}$$

Based on (2.12), the above expression can be reformed to:

$$\left(a_i - \sum_{k=-N}^{N} \alpha_k a_{i+k} \right) \cdot x = 0 \tag{2.16}$$

Vector a_i stands for the i^{th} row of matrix A in (2.13) and vector x stands for the original signal. As can be seen from the above two expressions, in order to meet (2.15), which denotes that each sample of a resampled signal can be represented by a linear combination of its 2N neighbors. The i^{th} row of A, denoted as a_i, should be equal to a linear combination of its 2N neighboring rows.

Since in practice, the resampling factor and the type of correlations are unknown, expectation/maximization algorithm (EM) is applied for estimation. Assuming each sample belongs to a certain state, which denotes that whether a sample is correlated to its 2N neighbors (*M1*) or not (*M2*). In E step of EM algorithm, the conditional probability is estimated, indicating whether a certain sample of the resampled signal belongs to *M1* or *M2*. By taking Bayes,

$$\Pr\{y_i \in M_i \mid y_i\} = \frac{\Pr\{y_i \mid y_i \in M_1\}\Pr\{y_i \in M_1\}}{\sum_{k=1}^{2}\Pr\{y_i \mid y_i \in M_k\}\Pr\{y_i \in M_k\}} \tag{2.17}$$

The prior probability $\Pr\{y_i \in M_1\}$ and $\Pr\{y_i \in M_2\}$ are assigned to 1/2 respectively. Moreover, $\Pr\{y_i \mid y_i \in M_1\}$ is assumed to be Gaussian with mean $\sum_{k=-N}^{N}\alpha_k a_{i+k}$ and $\Pr\{y_i \mid y_i \in M_2\}$ is treated as uniformly distributed.

In M step, the following quadratic error function is estimated:

$$E(\alpha) = \sum_i \omega(i)\left(y_i - \sum_{k=-N}^{N}\alpha_k y_{i+k}\right)^2 \tag{2.18}$$

The coefficient $\omega(i)$ is just $\Pr\{y_i \in M_1 \mid y_i\}$. To get the updated value of α, the derivative of (2.18) is taken and then set the result to zero. Therefore after the updated value of α is obtained in M step, it will be used in E step for the next loop. Similarly, after the updated value of $\omega(i)$ is obtained, in the following M step, it'll be used to calculate the coefficient α. EM algorithm is iteratively applied in this way

until it converges. As an intermediate result, $\Pr\{y_i \in M_1 \mid y_i\}$ is obtained to denote the probability of a certain sample being correlated to its neighbors. Figure 2.6 shows an example of the result calculated by EM algorithm.

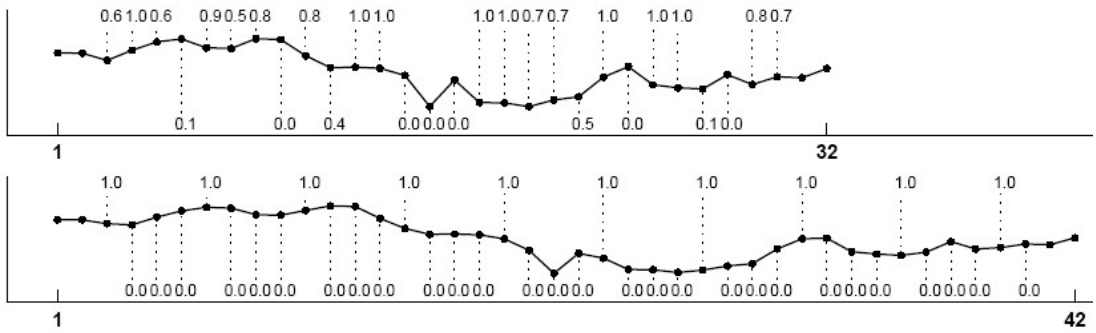


Figure 2.6 For each samples, the probability of being correlated to its neighbors are annotated. Period appears at up-sampled signal rather than original one. [19]

Experiments show that by using this basic framework, images tampered by resampling methods such as rotation or linear interpolation can be classified. But on the other hand, the weakness also exists and to be further improved. This method is applicable for only uncompressed images or JPEG and GIF images with tiny compression. Moreover, as will be discussed in Chapter 3, one anti-forensics method was developed to eliminate the linearity used within this method by applying a non-linear filter to the given image. Nevertheless, it is an effective technique that considers the basic principles of resampling and also has proven to be of great significance in tampering detection.

Finally, this algorithm considers the hidden states of those samples and uses EM algorithm to automatically update some information in an iterative way. A relatively more complicated technique is to be discussed in 2.2.3, which takes into account not

only the hidden state and EM algorithm, but also the hidden Markov models due to the statistical dependencies between wavelet coefficients across scales.

2.2.3 Discrimination between CG Images and Natural Images

As mentioned previously in this section, computer graphics (CG) techniques are being widely used as an effective way for image tampering. Thus discrimination between CG images and natural images are sure to be important in the field of tampering detection. In this section, a wavelet based hidden Markov model [20] is presented in details. Pan and Huang [21] utilized such model for discrimination between CG images and natural images. Dependencies between the states of neighboring wavelet coefficients are considered, which is not only used in tampering detection but actually many other fields like de-noising and signal detection.

The basic knowledge of discrete wavelet transform can be found in Appendix A. For wavelet transforms, there are two groups of properties which are primary properties and secondary properties. The primary properties are described as:

Locality: Each wavelet atom is localized simultaneously in time and frequency.

Multi-resolution: Wavelet atoms are compressed and dilated to analyze at a nested set of scales.

Compression: The wavelet transforms of real-world signals tend to be sparse

The secondary properties, composed of clustering property and persistence property, are particularly essential for this method since they act as the basic idea for those hidden Markov tree (HMT) models that consider the interdependencies across scales, which will be discussed later in this section. The secondary properties are

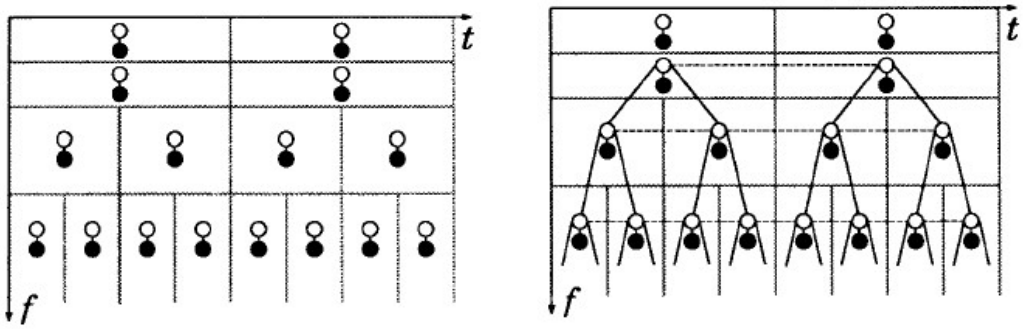
described as:

Clustering**:** If a particular wavelet coefficient is large/small, then adjacent coefficients are very likely to also be large/small.

Persistence: Large/small values of wavelet coefficients tend to propagate across scales.

Note that in this method, the dependencies considered are those of the states of wavelet coefficients rather than the values of the wavelet coefficients. Due to compression property, the coefficients of DWT consist of a small number of large coefficients and a large number of small ones. Then each wavelet coefficient is assigned a state, denoting whether the value of the wavelet coefficient is large or small. Since the states are unobserved, they are known as hidden states. Figure 2.7(a) illustrates such idea. In this image, each black dot represents a certain wavelet coefficient. Each white dot that is connected with a black dot denotes the hidden state of the coefficient.

Based on secondary properties, hidden Markov tree model is the statistical model used in this method. From Figure 2.7(b), the binary-tree structured is modeled to illustrate the interdependencies across scales.



(a) **(b)**

Figure 2.7 Shown are: (a) connection between wavelet coefficients and their hidden state; (b) binary tree structured models representing the interdependencies across scales. [20]

Each coefficient is modeled being in one of the two states: “High”, corresponding to those containing significant contributions of signal energy and “Low” to the opposite. As shown in Figure 2.8, for a certain wavelet coefficient, the PDF is a mixture Gaussian, which can be treated as the combination of a high-variance, zero-mean density and a low-variance, zero-mean density. Only the states of neighboring wavelet coefficients are linked together in the HMT model since locality and multi-resolution properties of DWT suggest that dependencies die off quickly as moving away from the local neighborhood about a coefficient of interest.

The state variable dependencies are modeled via state transition probability, which calculates the probability of the current state is “m” given the parent state is “r”. Generally speaking, using an M-state Gaussian mixture model for each wavelet coefficient Wi, the parameters for the HMT model, which can be further grouped into a model parameter vector θ are shown as:

$$[\ p_{S_1}(m),\ \varepsilon_{i,\rho(i)}^{m,r} = p_{Si|S_{\rho(i)}}[m|S_{\rho(i)}=r],\ \mu_{i,m},\ \sigma_{i,m}^2\ ] \qquad (2.19)$$

For parameter θ estimation, principle of maximum likelihood is applied. But due to the fact that states are hidden (unobserved), direct maximum likelihood estimation is intractable to estimate θ. Therefore expectation maximization (EM) algorithm is applied in order to iteratively update parameter θ and probabilities for hidden state S until it converges.

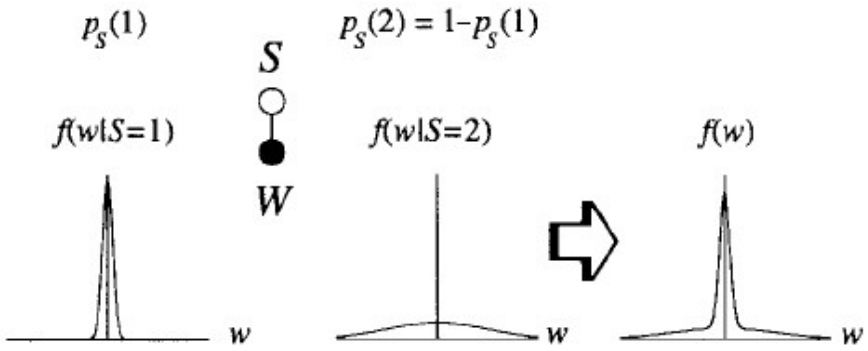


Figure 2.8 Two-states, zero-mean mixture Gaussian model for a certain wavelet coefficient. The black dot denotes the coefficient while the white dot represents the corresponding hidden state, with S = 1 representing a low-variance zero-mean Gaussian and S = 2 representing a high-variance zero-mean Gaussian PDF. [20]

The general idea is that in E step of EM algorithm, conditional probabilities of the hidden states are calculated, which are $p(S_i = m \mid \omega, \theta)$ and $p(S_i = m, S_{\rho_i} = n \mid \omega, \theta)$. By using forward-backward algorithm, these two probabilities can be represented using those parameters that form θ. Then in M step of EM algorithm, the updated values of the four elements that form θ are represented using those two conditional probabilities calculated during E step. In this way the value of the two conditional probabilities can be updated in the next loop. The E step and M step are iteratively repeated until it converges.

For discrimination between CG images and natural images, by using the model described above, F. Pan has applied machine learning techniques to discriminate CG images from natural images. Though LIBSVM and RBF kernel is used, the main idea is still based on the statistical model introduced before. Since zero-mean is assumed for the PDF of an arbitrary wavelet coefficient, the classification features are extracted from the other three elements other than mean value in (2.19).

Experiment results showed that for HSV color space, the classification accurate rate is close to 85%, which is a little better than that of RGB color space. It proves that HMT parameters are indeed effective classification features. Within this method, since it considers much about statistical relations between neighboring wavelet coefficients in a global view, it seems that such algorithm can be further applied to other related fields like steganalysis.

2.2.4 Tampering Detection using Statistical Wavelet Analysis

In 2.2.3 a technique based on DWT and HMM is shown in detail, in which statistical properties of DWT as well as hidden state of those wavelet coefficients are used. In contrast, another technique presented by H. Farid [22] directly considers the statistical relationship between the wavelet coefficients values rather than the hidden states.

The model of 2-D wavelet decomposition is shown as Figure 2.9, for more details about DWT please refer to Appendix A. Similarly to what has been discussed in Section 2.2.3, from [23], there exist correlations between the sub-band coefficients and their spatial or scale neighbors. A new amount which is linear predictor of coefficient magnitude is introduced here.

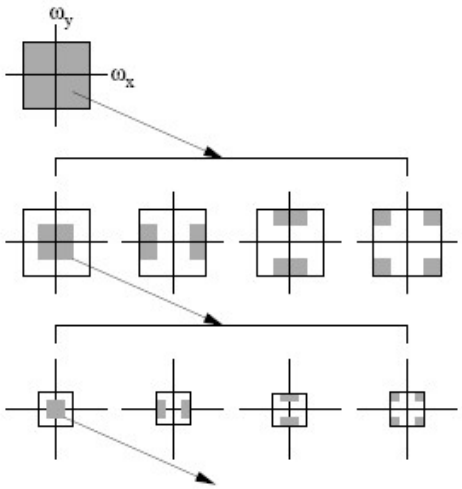


Figure 2.9 A multi-scale and orientation decomposition for wavelet transform. [23]

Due to the correlations mentioned above, let's consider either sub-band of the horizontal, vertical and diagonal sub-bands. Let's denote $V_i(x, y)$ as a vertical sub-band at scale i, which can be represented linearly by:

$$|V_i(x,y)|=\omega_1 |V_i(x-1,y)| +\omega_2 |V_i(x+1,y)| +\omega_3 |V_i(x,y-1)+\omega_3 |V_i(x,y+1)|$$

$$+\omega_5 |V_{i+1}(x/2,y/2)| +\omega_6 |D_i(x,y)| +\omega_7 |D_{i+1}(x/2,y/2)| \qquad (2.20)$$

This can be also written in matrix form as: $V = Q\omega$, where vector ω consists of coefficients from ω_1 to ω_7 and vector V contains the coefficient magnitudes. Then the coefficients vector ω can be obtained by minimizing the quadratic error function: $E(\omega) = \| V - Q\omega \|^2$. To achieve this, taking derivative of $E(\omega)$ and set the result to 0. In this way the coefficients vector ω can be determined. Finally the log error value is calculated which denotes the proportion between the actual coefficients and the predicted ones. Similarly to (2.20), the linear predictor for horizontal and diagonal sub-bands as well as the corresponding log error values can be obtained.

Then the coefficient statistics for horizontal, vertical and diagonal sub-bands as well as the corresponding log error values are to be used as the features for classification.

In the experiments, the authors not only used this model to test images, but also tried to figure out the outcomes if only one group of features, say coefficient statistics or error statistics, is used. It turns out that for some certain cases, only considering coefficient statistics is sufficient to get a considerable detection accuracy rate while for most of the cases, it is necessary to take the combination of those two types of features into consideration. The statistical model used within this technique that considers first and higher order wavelet statistics indeed can be widely used in digital image forensics since statistical correlations are examined. But on the other hand, statistical models are also vulnerable to anti-forensics method. It is because techniques can be easily applied to alter the statistical properties such as to make the higher order wavelet statistics of a tampered image consistent with those authentic ones.

CHAPTER 3

DETECTION OF DOUBLE JPEG COMPRESSION

JPEG is a commonly used method of lossy compression for image. When forger attempts to use software like Adobe Photoshop to edit a certain image, it will be re-saved after a series manipulation. Since most of the images are encoded using JPEG standard, if it is to be re-saved using JPEG again, it has been through double JPEG compression. This is also means that double quantization is performed. As can be imagined, if an image underwent double JPEG compression, it is very likely to be tampered. Although it is possible that the image has been compressed several times without being tampered, research on those artifacts that are brought about by double JPEG compression still became a crucial part of image forensics.

3.1 Main Procedure of JPEG Compression

JPEG lossy compression is a Discrete Cosine Transform (DCT) based process. In this scheme, image pixels are grouped into many non-overlapped 8 x 8 blocks firstly. And then 2-D DCT is performed on each 8 x 8 block. Then in frequency domain, the transformed image also contains many blocks of size 8 x 8. The totally 64 values within each block are known as DCT coefficients while the same position within those blocks is known as a mode. That is to say, in frequency domain, there are many 8 x 8 blocks and totally 64 modes. After DCT, those DCT coefficients are quantized based on a certain quantization table, which is also sized 8 x 8. Within this

quantization table, there are totally 64 values to be further processed on each mode, which is referred to as quantization steps. Note that most of the quantization steps within each quantization table are different from each other. The same mode within each block is to be processed with the same quantization step, which also illustrates the fact that such process is mode based. A standard quantization table is introduced by JPEG standard based on quality factor while in fact any one can create their own quantization table. The quality factor denotes the compression rate and quality of the image, with larger quality factor representing better quality as well as less compression rate and vice versa. After DCT and quantization, the last step is nothing but to transform the DCT coefficients that has been quantized into a bit stream by applying entropy coding like Huffman.

For decompression, the process is simply taking the inverse operations of the three steps mentioned above, which are DCT, quantization and entropy coding. Therefore in order to decompress an image, entropy decoding, dequantization and inverse DCT are consecutively applied. The main flow of the JPEG compression is shown in Figure 3.1.

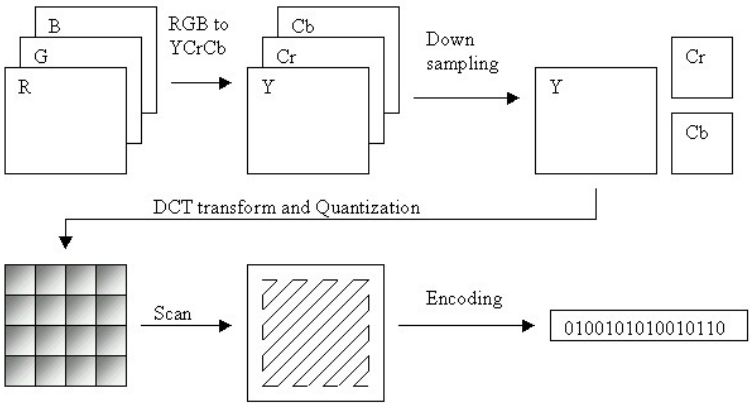


Figure 3.1 The flow chart for JPEG compression

3.2 Double Quantization

A JPEG image is said to be double-compressed if it has been through JPEG compression twice with different quantization steps. It is obvious that a double compressed JPEG image also underwent double-quantization process. Since the quantization steps used within those two quantization processes are different, some interesting properties are presented.

As mentioned in 3.1, for JPEG compression, 8 x 8 Block DCT is performed at the first stage. Then for each block, the DCT coefficients $c_{i,j}$ are quantized based on the quantization steps $Q^1_{i,j}$. After rounding process, the quantized coefficient is:

$$d_1 = \left[\frac{c_{i,j}}{Q^1_{i,j}} \right] \tag{3.1}$$

Here $[\bullet]$ denotes rounding. Then if the result is further quantized with another quantization step, firstly dequantize d_1 by multiplying $Q^1_{i,j}$ with d_1, and then quantize the result with quantization step $Q^2_{i,j}$, yielding double-quantized coefficients d_2:

$$d_2 = \left[\left[\frac{c_{i,j}}{Q^1_{i,j}} \right] \frac{Q^1_{i,j}}{Q^2_{i,j}} \right] \tag{3.2}$$

As shown above, double-quantization is equivalent to taking three steps in a row, which are quantization with step $Q^1_{i,j}$, dequantization with step $Q^1_{i,j}$ and quantization with step $Q^2_{i,j}$.

The theorem of the double compression artifacts based on the histogram of DCT coefficients is firstly represented by A. C. Popescu [24]. He analyzed the periodic artifacts in mathematical ways. Also in [25], [26], J. Lukas and J. Fridrich reported such periodic artifacts, along with three different methods for estimating the primary quantization matrix of a given image that underwent double JPEG compression. Figure 3.2 illustrates such periodic artifacts.

3.3 Some Techniques related to Double JPEG Compression

The importance of double JPEG compression detection drives many researchers to develop their own techniques and methods.

Hany Farid proposed a technique by evaluating JPEG ghost [27] to analyze double JPEG compression. Specifically, by using this method, compression history of different regions of an image is exposed. By evaluating the sum of squared differences between the DCT coefficients after single and double quantization, it is found that when quantization step $Q_{i,j}^{2}$ equals to $Q_{i,j}^{1}$, the difference will be minimal. If this idea is extended to triple-quantization with quantization step $Q_{i,j}^{3}$, when $Q_{i,j}^{3}$ equals to $Q_{i,j}^{1}$, the sum of squared difference reaches its minimum. Moreover, if $Q_{i,j}^{3}$ equals to $Q_{i,j}^{2}$, it reaches the second local minimum, which is defined as JPEG ghost. By evaluating this difference, this technique can successfully localize the corresponding tampered region of an image.

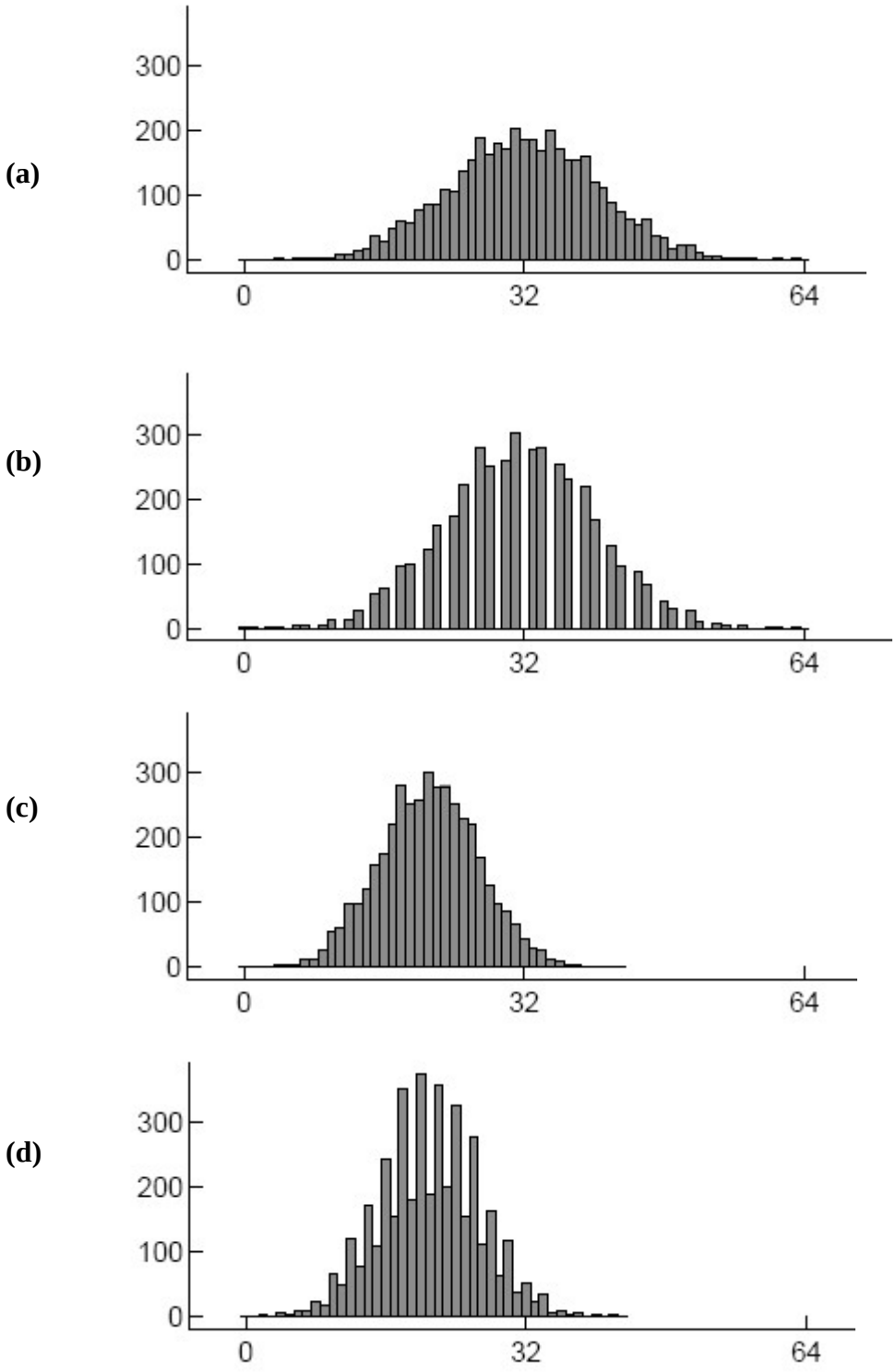


Figure 3.2 Periodic artifacts: (a) the histogram of single quantized signal with step 2; (b) the histograms of double quantized signals with step 3 followed by 2; (c) the histogram of single quantized signal with step 3; (d) the histograms of double quantized signals with step 2 followed by 3. As can be seen, the periodic artifacts are present only for double quantized signals rather than single quantized signals. [24].

Fu developed another algorithm for detection of double JPEG compression by using Benford's law [28], [29]. Benford's law, also known as first-digit law, states that the first digit is 1 about 30% of the time, and larger digits occur as the leading digit with lower and lower frequency [30]. From [31], the distribution of DCT coefficients is modeled as Laplacian distribution. Based on the generalized Benford's law developed by D. Fu, the distribution of the first digits of quantized DCT coefficients from those AC modes rather than DC mode are analyzed. The main idea is that double-quantization will make the distribution of the first digits against the generalized Benford's law, which can be used for double JPEG compression detection. Later, B. Li improved this effective technique to mode based first digit features [32], which achieved an outstanding accuracy rate for detection.

Besides local algorithms, there also exist some global algorithms that use machine learning technique to analyze double JPEG compression. C. Chen developed an algorithm [33] that firstly calculates the difference 2-D arrays of the DCT coefficients along horizontal, vertical, main diagonal and minor diagonal directions respectively. Then after setting threshold values to the difference 2-D arrays, transition probability matrix is used to extract the features for classification. The difference 2-D arrays of DCT coefficients as well as the transition probability matrix are involved in the technique discussed in 2.2.1 as well.

Moreover, by measuring inconsistencies of blocking artifact, S. Ye proposed a method for double JPEG compression detection [34]. Interestingly, by using Fourier, the second order derivative of the power spectra of DCT coefficients histogram is

calculated, which is relatively rare since other transforms like DCT and wavelet are widely used in the field of tampering detection rather than Fourier analysis. But on the other hand, the histogram model mentioned within this method is more likely to be double quantized rather than single quantized and hence the periodic artifacts may not be exactly the same as described in the paper. Therefore further investigation is inevitable.

3.4 Anti-Forensics Techniques related to Double JPEG Compression

As described previously, several different methods are developed for double JPEG compression detection based on the artifacts brought about by double quantization. On the other hand, some techniques are generated to reduce such artifacts to prevent from detecting double JPEG compression. Although for the image forensics techniques mentioned above, the authors have listed some corresponding limitations or even drawbacks. In recent years, a new field was raised that aims at fighting against those image forensics techniques, which is known as anti-forensics. Specifically, a group of researchers from University of Maryland developed several methods for anti-forensics, especially focusing on some existing methods for double JPEG compression detection.

Stamm et al. and other members from University of Maryland have published several articles that are related to anti-forensics [35], [36], [37]. Such study not only shows the vulnerability of existing image forensics techniques, but also accelerates the improvement of image forensics methods. The method Stamm developed is to add

anti-forensic dither, which is additive white noise, to the transform coefficients [37]. To set up the generalized framework of such method, firstly the distribution of the transform coefficients of an image before compression is estimated. Then after compression, no matter JPEG or wavelet compression, anti-forensics dither is added to the transform coefficients. By processing in this way, the distribution after compression matches the estimated distribution of the previous step. The aim of such method is to make the transform coefficients distribution more likely to be an uncompressed one. Moreover, to eliminate the blocking artifacts of double JPEG compression, a median filter is applied and then anti-forensic dither is further added to the result [35].

On the other hand, in previous section, the detection of double JPEG compression using Benford's law is introduced. Wang et al. [38] used the technique of histogram equalization to make the result satisfying Benford's law even for double quantization, which represents the limitations of Benford's law when applying to double JPEG compression detection.

As discussed, the technique based on Markov transition probability is a relatively ideal way for double JPEG compression detection since it considers a lot about statistical correlations. But on the other hand, by adding some noise, similarly to the anti-forensics dither, it may modify more or less the overall statistical properties of a given image. Therefore probably it may result in inaccurate classification outcomes. But until now, there's no paper published to attack this Markov based method yet.

Once a successful image forensics technique has been developed, there will be

corresponding anti-forensics method that is used to attack the former one. For example, as discussed in Section 2.2.2, by evaluating the linear relationship between a number of signal samples, image tampering manipulations such as rotation, resizing or stretching can be detected. But if the image is further processed with a nonlinear filter, then the artifacts won't represented any more, as described in [39] by Kirchner. Forensics and anti-forensics are sure to endlessly fight against each other. But on the other hand, thanks to those anti-forensics techniques, more and more mature forensics methods are being developed.

CHAPTER 4

CONCLUSION

Digital image forensics is a passive way to protect the authenticity and integrity of an image, unlike other active ways such as digital watermarking or steganography. Actually digital image forensics is a relatively broad topic, which includes several different realms such as tampering detection, source identification and double JPEG compression detection. Although some people may think double JPEG compression detection belongs to tampering detection, there still exist some differences between the two topics and obviously the main difference is that an image that has been through double or even more times JPEG compression may not be tampered. But detection of double JPEG compression still acts as an important role in image forensics, with no doubt.

For double JPEG compression detection, as mentioned previously, the direct way is to evaluate the mode histogram of the block DCT coefficients. Periodic artifacts are presented if an image has undergone double quantization, which is not possible for single quantization. But such method also has its limitations such as the case when the second quantization step is the multiple of the first one. Therefore other algorithms based on Benford's law or transition probability matrix are developed. Due to the consideration of statistical correlations as well as the use of machine learning techniques for classification, the transition probability based technique has reached a satisfying accuracy rate and also appears to be a relatively ideal way for

detection of double JPEG compression.

Furthermore, though image forgeries may fool human eyes, any manipulation applied to digital images changes image statistics. Therefore identifying statistical artifacts becomes critically important in image forensics. Signal processing tools such as wavelet transform, hidden Markov models and statistical moments are used in various different techniques for both tampering detection and double JPEG compression, as mentioned in Chapter 2 and Chapter 3.

Image forensics is a relatively new topic compared to other signal processing related fields and the techniques developed in recent years are highly dependent on the previous research. For example in 1998, the idea of wavelet-based statistical signal Processing using HMM is developed by Matthew Crouse and Robert Nowak [20], which was further applied to image forensics since recent years, as mentioned in Section 2.2.3. Until now, image forensics techniques are far from mature and actually highly dependent on the image database being used, which seems to be one of the bottlenecks that need to be improved. There are several well-known image datasets for researchers to use such as Columbia Image Splicing Detection Evaluation Dataset. But when it comes to practical use, it is still a long way to apply most of the techniques into a randomly selected digital image. But just as the rapid increasing number of related paper during the last several years, not only the rising extensive activities can be envisionedrelated to digital image forensics but also the increasing matured techniques that are independent of the images being used

APPENDIX A

BRIEF INTRODUCTION OF DISCRETE WAVELET TRANSFORM [40]

Similarly to Fourier Transform, instead of using sine and cosine wave as the basis, wavelet transform represents a certain signal in terms of shifted and dilated versions of a prototype wavelet function. There are two different functions that are very essential for wavelet transform, which are scaling function and wavelet function. It will be shown below how they acted in wavelet transform and how discrete wavelet transform (DWT) is applied to 2-D images.

The scaling function is denoted as $\varphi(t)$. Then define:

$$\varphi_{j,k}(t) = 2^{j/2}\varphi(2^j t - k) \tag{A.1}$$

Here j represents the scales and $\varphi_{j,k}(t)$ is the dilated and shifted version of $\varphi(t)$ in which j is the parameter in frequency domain while k, a parameter in time domain, represents the shifted amount. This also illustrates how wavelet transform can be evaluated in both time and frequency domain simultaneously. Here, as scale goes up, the higher resolution is obtained. Since $\varphi_{j,k}(t)$ is "narrower" than $\varphi_{j-1,k}(t)$, in time domain, $\varphi_{j,k}(t)$ can be used to represent more signals, which means that the signal space of $\varphi_{j,k}(t)$ is larger than that of $\varphi_{j-1,k}(t)$, which also means that if signal x(t) can be linearly represented by $\varphi_{j-1,k}(t)$, it is also with $\varphi_{j,k}(t)$. Therefore lower resolution signal can be linearly represented by higher resolution signal.

The multi-resolution function of scaling function $\varphi(t)$ is defined as:

$$\varphi(t)=\sum_{n} h_0[n]\sqrt{2}\varphi(2t-n) \tag{A.2}$$

Here $h_0[n]$ is the scaling function coefficient and the relationship between the scaling functions of neighboring scales can be evaluated.

Similarly to scaling function, the wavelet function which is denoted as $\psi_{j,k}(t)$ can be represented by:

$$\psi_k(t)=2^{j/2}\psi(2^j t-k) \tag{A.3}$$

Generally, $\psi_{j,k}(t)$ and $\varphi_{j,k}(t)$ are orthogonal, which means:

$$\left\langle \varphi_{j,k}(t),\psi_{j,l}(t)\right\rangle = \int \varphi_{j,k}(t),\psi_{j,l}(t)dt = 0 \tag{A.4}$$

Still, similarly to scaling function case, the multi-resolution function for wavelet function $\psi(t)$ is represented as:

$$\psi(t)=\sum_{n} h_1[n]\sqrt{2}\psi(2t-n) \tag{A.5}$$

Here $h_1[n]$ is known as the wavelet coefficient and the relationship between scaling coefficient and corresponding wavelet coefficient is:

$$h_1[n]=(-1)^n h_0[1-n] \tag{A.6}$$

When it comes to decomposition, input signal x(t) can be decomposed into two parts, which are the scaling function $\varphi_{j,k}(t)$ which denotes the coarse information of the signal, and the wavelet function $\psi_{j,k}(t)$ that represents the fine information of the signal. If 1-D DWT is extended to 2-D case, given a certain image f(x,y), firstly f(x,y) is analyzed along x direction using $\varphi(x)$ and $\psi(x)$ respectively and two sub-bands are obtained, which denote the fine information along x direction and the coarse information along x direction respectively. Then we further analyze the two sub-bands signals along y direction using $\varphi(y)$ and $\psi(y)$. Finally four different sub-bands are obtained, which are LL (Low-Low), LH (Low-High), HL (High-Low) and HH (High-High).

REFERENCES

[1] Wikipedia: http://en.wikipedia.org/wiki/Brian_Walski Retrieved April 29th, 2011

[2] Y. Shi, C. Chen, G. Xuan and W. Su (2008). Steganalysis versus splicing detection. *IWDW '07: Proceedings of the 6th International Workshop on Digital Watermarking*

[3] J. A. Redi, W. Taktak and J. Dugelay (2011). Digital image forensics: a booklet for beginners. *Multimedia Tools and Applications , Volume 51 Issue 1*

[4] Y. Shi, C. Chen and W. Chen (2007). A natural image model approach to splicing detection. *ACM Multimedia and Security Workshop*

[5] Wikipedia: http://en.wikipedia.org/wiki/Digital_watermarking Retrieved April 29th, 2011

[6] Wikipedia: http://en.wikipedia.org/wiki/Steganography Retrieved April 29th, 2011

[7] Y. Shi, C. Chen and W. Chen (2006). A Markov process based approach to effective attacking JPEG steganography. *Information Hiding Workshop (IHW06*)

[8] Y. Shi, G. Xuan, D. Zou, J. Gao, C. Yang, Z. Zhang, P. Chai. W. Chen and C. Chen (2005). Steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image and neural network. *IEEE International Conference on Multimedia and Expo (ICME05)*

[9] C. Chen, Y. Shi and G. Xuan (2007). Steganalyzing texture images. *IEEE International Conference on Image Processing (ICIP07)*

[10] D. Fu, Y. Shi and W .Su (2006). Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition. *International Workshop on Digital Watermarking (IWDW06)*

[11] http://www.digitalphotomakeover.com/photopeopleremoval.html Retrieved April 29th, 2011

[12] M. Bertalmio and G. Sapiro (2000). Image inpainting. *Proceedings of SIGGRAPH*

[13] http://cg.yin10.com/news/cgnews/2007/114/07-1-14-1-40-2-I7E46.htm Retrieved April 29th, 2011

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

[15] A. C. Popescu and H. Farid (2004). Exposing digital forgeries by detecting. duplicated image regions. *Department of Computer Science, Dartmouth College, Tech. Rep.* TR2004-515

[16] T-T. Ng and S-F. Chang (2004). A model for image splicing. *IEEE International Conference on Image Processing*

[17] S. Lyu and H. Farid (2002). Detecting hidden messages using higher-order statistics and support vector machines. *Information hiding: 5th international workshop*

[18] D. Zou, Y. Shi, W. Su and G. Xuan (2006). Steganalysis based on Markov model of thresholded prediction-error image. *In Proc. of IEEE International. Conference on Multimedia and Expo,* pp 1365-1368

[19] A. Popescu and H. Farid (2005). Exposing digital forgeries by detecting traces of resampling. *IEEE Transactions on Signal Processing*

[20] M. S. Crouse, R. D. Nowak and R. G. Baraniuk (1998). Wavelet-based statistical signal processing using hidden Markov models. *IEEE Trans. Signal Processing,* vol. 46, pp. 886–902

[21] F. Pan and J. Huang (2010). Discriminating computer graphics images and natural images using hidden Markov tree model. *IWDW '10: International Workshop on Digital Watermarking,* pp. 23-28

[22] H. Farid and S. Lyu (2003). Higher-order wavelet statistics and their application to digital forensics. *IEEE Workshop on Statistical Analysis in Computer Vision*

[23] R. Buccigrossi and E. Simoncelli (1999). Image compression via joint statistical characterization in the wavelet domain. *IEEE Transaction on Image Processing, Vol. 8, No. 12*

[24] A. C. Popescu (2005). Statistical tools for digital image forensics. *Ph.D. thesis,* Department of Computer Science, Dartmouth College

[25] J. Lukas and J. Fridrich (2003). Estimation of primary quantization matrix in double compressed JPEG images. *Proc. of DFRWS*

[26] T. Pevny and J. Fridrich (2008). Estimation of primary quantization matrix for steganalysis of double-compressed JPEG images. *Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia*

[27] H. Farid (2009). Exposing digital forgeries from JPEG ghosts. *IEEE Transactions on Information Forensics and Security , Volume 4 Issue 1*

[28] D. Fu, Y. Shi and W. S (2007). A generalized Benford's law for JPEG coefficients and its applications in image forensic. *in Proc. SPIE, Security, Steganography and Watermarking of Multimedia Contents*

[29] D. Fu, H. Zhang and Y. Shi (2006). A generalized Benford's law for JPEG coefficients. *Technical Report,* Department of Electrical and Computer Engineering, New Jersey Institute of Technology

[30] Wikipedia: http://en.wikipedia.org/wiki/Benford%27s_law Retrieved April 29th, 2011

[31] R. C. Reininger and J. D. Gibson (1983). Distributions of the two dimensional DCT coeffcients for images. *IEEE Trans. On Commun., Vol. Com-31,* pp835-839

[32] B. Li, Y. Shi and J. Huang (2008). Detecting double compressed JPEG images by using mode based first digit features. *IEEE International Workshop on Multimedia Signal Processing (MMSP08),* pp.730-735

[33] C. Chen, Y. Shi and W. Su (2008). A machine learning based scheme for double JPEG compression detection. *IEEE International Conference on Pattern Recognition (ICPR08)*

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

[35] M. C. Stamm, S. K. Tjoa, W. Lin and K. Liu (2010). Undetectable image tampering through JPEG compression anti-forensics. *IEEE Int'l Conf. Image Processing (ICIP)*

[36] M. C. Stamm and K. Liu (2010). Anti-forensics of digital image compression. *IEEE Trans. on Information Forensics and Security, vol. 6, no. 2*

[37] M. C. Stamm and K. J. R. Liu (2010). Wavelet-based image compression anti-forensics. *IEEE Int'l Conf. Image Processing (ICIP)*

[38] J. Wang, B. Cha, S .Cho and C. Jay (2009). Understanding Benford's law and its vulnerability in image forensics. *in Proc. IEEE International Conference on Multimedia and Expo, MSATC,* pp. 1568—1571

[39] M. Kirchner and R. Bohme (2008). Hiding traces of resampling in digital images. *IEEE Transactions on Information Forensics and Security. Vol. 3, no. 4,* pp. 582-592

[40] A. N. Akansu and R. A. Haddad (1992). Multiresolution signal decomposition: transforms, subbands, and wavelets. *Boston, MA: Academic Press,* ISBN 978-0-12-047141-6

[41] S. Lyu and H. Farid (2005). How realistic is photorealistic? *IEEE Transactions on Signal Processing, vol. 53, issue 2,* pp. 845-850

[42] Wikipedia: http://en.wikipedia.org/wiki/Hidden_Markov_model Retrieved April 29th, 2011

[43] Z. Lin, J. He, X. Tang and C. Tang (2009). Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. *Pattern Recognition, Vol. 42, No. 11,* pp. 2492-2501