Image forensics on exchangeable image file format header

Fan, Jiayuan

2014

Fan, J. (2014). Image forensics on exchangeable image file format header. Doctoral thesis,
Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/61970>

<https://doi.org/10.32657/10356/61970>

Image Forensics on Exchangeable Image File Format Header

Jiayuan Fan
School of Electrical and Electronic Engineering
2014

Image Forensics on Exchangeable Image File Format Header

Jiayuan Fan

School of Electrical and Electronic Engineering

A thesis submitted to the Nanyang Technological University
in partial fulfillment of the requirement for the degree of
Doctor of Philosophy

2014

Acknowledgements

First, I would like to express my deep and sincere thanks to my PhD supervisor, Professor Alex C. Kot, for supporting me during these past five years. It has been an honor to be his PhD student and supervised by him. He has taught me, both consciously and un-consciously, how good research work should be done. He has provided numerous ideas, and invaluable time to support my research. His forward-looking advice, endless patience, continuous encouragement and guidance, has made my Ph.D. experience more productive and stimulating, and also make the thesis possible. He has been a supportive advisor, and has given me the freedom to pursue independent work without objection. Especially, when I experienced some tough times in the PhD pursuit period, his research passion and enthusiasm can always inspire me to conquer those difficulties, and was contagious and motivational for me. I gain not only the professional knowledge from him but also the way of thinking and solving a problem. I am sure what I have gained from him will benefit me in my future life.

The members of Prof Kot's group have contributed immensely to my personal and professional life in Nanyang Technological University. The group members always maintain deep friendships and good collaboration. I would like to thank Dr Cao Hong for providing detailed and great advice during our collaboration process. His helpful suggestions have helped me a lot. Other group members that I have had the pleasure to work with are Dr Li Sheng, Dr Liu Siyuan, and Dr Chen Changsheng. I would like to thank them all for their positive suggestions and concerns for my work. Their thoughtful comments and encouragement are highly appreciated. I also would

like to thank all the members and staff of the workstation resource laboratory for providing me with a comfortable and pleasant working environment when I am doing my research.

I would like to thank my parents for their persistent support and care all these years. Without their education and sacrifice, I would never have an opportunity to pursue the postgraduate degree without worries. I am grateful to my brother for his continuous support and encouragement, especially no matter what I choose to do.

Last but not least, this thesis is dedicated to my husband Dr Chen Tao and my son for their endless love. It is they who always believe me and support me. Without them, I would never have a happy life.

Table of Contents

Acknowledgements	i
Table of Contents	iii
Summary	viii
List of Figures	xi
List of Tables	xvii
List of Abbreviations	xix
1 Introduction	1
1.1 Motivation	1
1.2 Overview of Image Forensics	3
1.2.1 Image Forensics Issues	3
1.2.2 Image Forensics Categories	6
1.3 Overview of EXIF	7
1.3.1 EXIF History	7
1.3.2 EXIF Structure	8

1.3.3	EXIF Related Application	10
1.4	Major Contributions	12
1.5	Organization of This Thesis	15
2	Background and Literature Review	17
2.1	Digital Still Camera System	17
2.2	Current Passive Forensics Evidences	18
2.2.1	Scenery Regularities	19
2.2.2	Optical Regularities in Optical Lens	21
2.2.3	Sensor Imperfections	23
2.2.4	Processing Regularities in The Digital Processing Unit	25
2.2.5	Generic Statistical Regularities	27
2.2.6	EXIF-based Prior Works	27
2.3	Comparison of Different Evidences	28
2.4	Summary	31
3	Exploring The Novel Evidence for Image Forensics Analysis	32
3.1	Introduction	32
3.2	Image Noise Associated with Camera Settings in EXIF	33
3.2.1	Image Visual Noise Pattern	33
3.2.2	Photon Transfer Curve	34

3.2.3	Camera Settings from The EXIF Header	36
3.3	Proposed Method	39
3.3.1	Extraction of Image Noise Features	39
3.3.2	Extraction of EXIF Header Features	43
3.3.3	Modeling The EXIF-Image Correlation in Linear Regression .	44
3.3.4	Detection of Image Manipulation	46
3.4	Experiments and Results	47
3.4.1	Dataset	48
3.4.2	Image Tampered by Brightness and Contrast Adjustment . . .	49
3.4.3	Manipulation Detection on An Individual Camera	52
3.4.4	Manipulation Detection on Different Camera Brands and Models	54
3.4.5	Detection of Mixed Manipulation Types	55
3.5	Summary	56
4	Estimating EXIF Parameters for Image Manipulation Detection	57
4.1	Introduction	57
4.2	Proposed Manipulation Detection Framework	59
4.2.1	Extraction of Image Noise Features	60
4.2.2	Extraction of EXIF Header Features	61
4.2.3	Modeling the EXIF-Image Correlation in Non-linear Regression	61

4.2.4	Image Manipulation Detection	64
4.3	Experiments and Results	65
4.3.1	Detection of Individual Manipulation Curve	65
4.3.2	Refining The EXIF Header Features	81
4.3.3	Manipulation Detection without Knowing The Camera Source	82
4.3.4	Detection of Forgery Photos	85
4.3.5	Countering Anti-forensics Threat	86
4.4	Summary	92
5	EXIF-White Balance Recognition for Image Forensics Analysis	94
5.1	Introduction	95
5.2	Background	97
5.3	Proposed Detection Framework	99
5.3.1	White Balance Algorithms for Image Quality Metrics	99
5.3.2	Eigen Feature Regularization	102
5.3.3	Image Forensics Analysis	106
5.4	Experiments and Discussion	107
5.4.1	EXIF-White Balance Recognition on Compressed Images	107
5.4.2	Determining EXIF-White Balance Levels on Resized Images	112
5.4.3	Detection of Forgery Photos	113

Table of Contents

5.4.4	Investigation of Auto and Sunny White Balance Levels	118
5.4.5	Anti-forensics Threat Discussion	119
5.5	Summary	120
6	Conclusions and Future Works	121
6.1	Conclusions	121
6.2	Future Works	123
	Author's Publications	125
	References	126

Summary

In recent years, technologies related to digital photography including both hardware and software have gained rapid progress. As a result of these technologies' wide application in digital still camera (DSC) system, many researchers become increasingly interested in using the digital cameras to record the real happenings for supporting evidences and historical events, such as news reporting in journal and magazine, police investigation and law enforcement, etc. The digital images as the outputs of digital cameras, can record these events. However, accompanied with these emerging digital photography technologies, various kinds of image editing tools have also been developed. With these tools, digital images can be easily altered without any visual clues left. As a result, the credibility of digital images becomes questionable. For example, when a forged photo is adopted as the court judgment evidence, incorrect verdict may happen. In view of this, this thesis focuses on passive image forensics research which uses both the Exchangeable Image File Format (EXIF) information and the image captured by a camera to verify the authenticity and integrity of the digital image.

In Chapter 3, a novel evidence by using the EXIF information for image forensics task is explored. Five EXIF header features including aperture, shutter speed, ISO speed rating, brightness value and exposure are correlated with the image statistical noise features. The linear regression algorithm is used to model the relationship between each EXIF header feature and the image statistical noise features. The sequential forward feature selection (SFFS) is adopted to select the significant noise features for each EXIF parameter estimation. The experimental results show the

effectiveness of involving EXIF information for image forensics analysis.

In Chapter 4, a new manipulation detection method by using the nonlinear regression algorithm to model the correlation between refined EXIF header features and image statistical noise features is developed. The refined EXIF header features include only aperture, shutter speed and ISO speed rating for computation, where brightness value and exposure are removed due to their linear correlation and little performance gain for manipulation detection. Through this, the redundant computation is avoided. By further investigating the correlation between statistical noise features and three EXIF header features, the nonlinear regression algorithm is developed to establish the EXIF-Image model. The generated numerical difference in the modeling process is also used as a manipulation indicator, which achieves excellent performance in detecting the common brightness and contrast adjustment. The proposed manipulation detection is also demonstrated to work well in a blind mode, where the camera brand and model sources are unavailable.

In Chapter 5, an image tampering detection approach by exploiting EXIF-white balance parameter is developed. For each white balance level in the EXIF, the image quality metrics (IQM) features between every pair of the original image and its re-balanced image are first extracted. The image eigen decomposition is then adopted to generate a compact set of discriminative features. The support vector machine (SVM) is finally employed to train these discriminative features into a classifier for each white balance level. These SVM models will be used to classify a new test image and give its belonged white balance level, which is then compared with white balance recorded in the EXIF for image tampering detection. Through experiments, our proposed approach is found to be able to detect complex image tampering, i.e. copy-and-paste followed by the high compression.

We validate the proposed algorithms and techniques on several image databases, including the database which contains the images from three different camera brands and models with various camera settings in the EXIF header, and the dataset consist-

ing of images from three different camera brands with multiple white balance levels. The experimental results on these databases consistently show the effectiveness of the proposed methods for image forensics analysis. Furthermore, the comparison with other state-of-the-art techniques indicates that the proposed algorithms achieve better performance in terms of the true positive (TP) and true negative (TN) rates.

As the research in passive image forensics continues searching for good and intrinsic evidences for exposing the presence of image forgeries, the significant results achieved by using our proposed methods demonstrated a new possibility to model the underlying scenarios between the image and its metadata entries for reliable forensics analysis.

List of Figures

1.1	Two cases of doctored photos [1]. (a) O.J. Simpson murder case. (b) A US air force helicopter and shark.	2
1.2	An example of a photo with its EXIF header information.	3
1.3	History of EXIF evolution (courtesy from [2])	7
1.4	Basic structure of uncompressed data files (courtesy from [3])	9
1.5	Basic structure of compressed data files (courtesy from [3])	10
1.6	A suggested framework of modeling various EXIF-Image correlations	12
2.1	The pipeline of the DSC system	18
3.1	Visual noise comparison for images captured of the same scenery by a Canon 550D camera with different ISO speed ratings. (a) Ground-truth scenery. Captured images (b) with ISO=800; (c) with ISO=3200 and (d) with ISO=12800. f-number and exposure time are fixed at 4.5 and $\frac{1}{60}$ second.	34
3.2	Process of converting light signals into digital signals in a DSC system.	35
3.3	Photon transfer curve.	35

3.4	Images of the same scene captured with exposure time decreased by one full <i>stop</i> and other settings unchanged. Top row from left to right: exposure time = 15, 8, 4. The middle row from left to right: exposure time = 2, 1, $\frac{1}{2}$. Bottom row from left to right: exposure time = $\frac{1}{4}$, $\frac{1}{8}$, $\frac{1}{15}$.	36
3.5	A small f-number as shown in top row and a big f-number as shown in the bottom row (courtesy from [4])	37
3.6	Images of the same scene captured with f-number changed by one full <i>stop</i> and other settings unchanged. Top row from left to right: f-number = 2.8, 4.0, 5.6. Bottom row from left to right: f-number = 8.0, 11, 16.	38
3.7	Images of the same scene captured with ISO speed rating increased by one full <i>stop</i> and other settings unchanged. The row from left to right: ISO = 100, 200, 400.	38
3.8	Modeling the correlation between images and each EXIF header feature in the linear regression	39
3.9	An example of the sharp area in the histogram distribution of the edge magnitude signal of the image. (a) A Photo (b) The sharp area in the histogram distribution of the edge magnitude signal regarding the image (a)	40
3.10	An example of the sharp edge area before and after dilating the grayscale image. (a) Before dilation (b) After dilation	40
3.11	RMSRE versus selected features number in SFFS for estimating aperture value.	45
3.12	Detecting image manipulation using each of EXIF header features. . .	47
3.13	Some samples of three different camera images.	48

3.14	Camera setting distributions of the dataset. (a) Aperture value distribution (b) Shutter speed value distribution (c) ISO speed rating value distribution (d) Brightness value distribution (e) Exposure value distribution	49
3.15	Mapping curves used for brightness and contrast adjustment.	51
3.16	Some examples of an image tampered by brightness and contrast adjustment curves. Images tampered by (a) Brightness increment, (b) Brightness decrement, (c) Gamma expansion, (d) Gamma compression, (e) S curve, (f) Inverse S curve.	52
3.17	ROC curve of five EXIF header features.	53
4.1	Extraction of image statistical noise features.	60
4.2	Block diagram of the proposed method.	62
4.3	Brightness and contrast adjustment with small changes.	66
4.4	Fisher's Ratio distributions against number of selected features for estimating aperture value in terms of different curves of (a) Brightness decrement (b) Gamma expansion (c) S curve.	67
4.5	The numerical difference distributions of the intact testing images and the manipulated testing images of Brightness decrement in (a), Gamma expansion in (b), S curve in (c).	68
4.6	Zoomed-in ROC curves for EXIF aperture value corresponding to six curves of brightness and contrast adjustment.	70

4.7	Aperture predictions for the images from the same camera with the equivalent DCSI by varying different settings of aperture value (Av) and shutter speed value (Sv), respectively. Aperture predictions for (a) intact images and (b) manipulated images by brightness decrement.	73
4.8	Shutter speed predictions for the images from the same camera with the equivalent DCSI by varying different settings of aperture value (Av) and shutter speed value (Sv), respectively. Shutter speed predictions for (a) intact images and (b) manipulated images by brightness decrement.	74
4.9	Aperture predictions for the images from different cameras with the equivalent DCSI by varying different settings of aperture value (Av) and shutter speed value (Sv), respectively. Aperture predictions for (a) intact images and (b) manipulated images by brightness decrement.	76
4.10	Shutter speed predictions for the images from different cameras with the equivalent DCSI by varying different settings of aperture value (Av) and shutter speed value (Sv), respectively. Shutter speed predictions for (a) intact images and (b) manipulated images by brightness decrement.	77
4.11	Sensitivity analysis of manipulation detection performance for $G_1(g, \beta)$, $G_2(g, \gamma)$, $G_3(g, \alpha)$ and $G_3^{-1}(g, \alpha)$ curves.	78
4.12	Images (a-i) with f-number = 5.6, exposure time = $\frac{1}{250}$, ISO = 400. Manipulated images (a-d) and (f-i) are generated from intact image (e) by image brightness changes of $G_1(g, \frac{1}{4})$, $G_1(g, \frac{1}{8})$, $G_1(g, \frac{1}{16})$, $G_1(g, \frac{1}{32})$, $G_1(g, -\frac{1}{32})$, $G_1(g, -\frac{1}{16})$, $G_1(g, -\frac{1}{8})$ and $G_1(g, -\frac{1}{4})$	80

4.13	Manipulated image (b) is generated from intact image (a) by “Brightness decrement”. Composite images (d) and (f) are created by intact images (c) and (e).	84
4.14	Photo (a) with f-number = 2.8, exposure time = $\frac{1}{125}$, ISO = 100; (b) with f-number = 4.0, exposure time = $\frac{1}{1000}$, ISO = 800.	88
4.15	Images are captured of the same scenery by an Olympus E500 camera with different settings of f-number. (a) f-number = 2.8. (b) f-number = 8. Exposure time and ISO are fixed at $\frac{1}{125}$ second and 100.	90
4.16	The block areas are chosen from the green color channel of the captured images.	91
4.17	Fitting the mapping curve from the block areas of Figure 4.16(a-b). .	92
4.18	The manipulated image resulted from Figure 4.16(a) by the fitting mapping curve.	92
5.1	Photos are taken of a plain white piece of A4 printer paper indoor on the board under the white fluorescent strip light tubes by Canon 550D with f-number = 5.6, exposure time = $\frac{1}{200}$, and ISO = 6400.	98
5.2	Block diagram of the proposed method.	99
5.3	Eigen spectra of IQM feature set of the training images with QF=20 including three different white balance levels, and the regularized eigen spectra.	103
5.4	Eigen spectra and zoomed version of the total covariance matrix after the whitening transformation.	105
5.5	Some photo samples from Canon 550D camera.	107

5.6	SVM scores against the number of selected features for (a) the original and (b) compressed training images with QF=20.	109
5.7	Manipulated images (b) and (d) are generated from intact image (a) and (c) by white balance post-processing.	114
5.8	Manipulated image (c) is generated from intact images (a-b) by copy-and-paste followed by white balance post-processing.	115
5.9	Manipulated images (d-f) are generated from intact images (a-c) by copy-and-paste followed by compression operation with QF of 70, 50 and 20. Manipulated images (g-i) are created from intact images (a-c) by copy-and-paste followed by downsampling of $\frac{1}{2}$, $\frac{1}{4}$ and $\frac{1}{8}$	116
5.10	Images (a-b) are taken outdoor with auto and sunny white balance respectively. Images (c-d) are taken indoor with auto and sunny white balance respectively.	119
6.1	Framework for future work	123

List of Tables

2.1	Comparison of Different Evidences	29
3.1	Key parameters of three cameras.	47
3.2	The performance of Olympus E500 camera for five EXIF header features.	54
3.3	Accuracy rate for different EXIF header features on multiple cameras	55
4.1	The performance comparison for different manipulation curves.	69
4.2	The performance comparison for the images from fixed camera settings.	71
4.3	EXIF parameter estimation for the photos in Figure 4.12.	80
4.4	The performance comparisons.	81
4.5	The performance comparison for the images from different camera sources.	83
4.6	Performance comparison for the images for modeling from one camera brand and the testing images from the other camera brand.	83
4.7	EXIF parameter estimation for the images in Figure 4.13.	86
4.8	EXIF parameter estimation for the photos in Figure 4.14	89

5.1	Overview of different white balance algorithms.	100
5.2	Image quality metrics feature pool.	101
5.3	Key parameters of three different cameras.	106
5.4	The performance comparison for the original and compressed images from different camera sources.	110
5.5	The performance comparison for the compressed images from different camera sources.	111
5.6	The performance comparison for the resized images from different came sources.	112
5.7	EXIF white balance prediction for the images in Figure 5.7-5.9. . . .	117
5.8	The performance comparison for the original images from Canon camera.	118

List of Abbreviations

APP	Application Market Segment
CCD	Charge Coupled Device
CFA	Color Filter Array
CMOS	Complementary Metal Oxide Semiconductor
CRF	Camera Response Function
DCSI	Digital Camera Signal Intensity
DSC	Digital Still Camera
DSLR	Digital Single Lens Reflex
EXIF	Exchangeable Image File Format
FP	False Positive
GIF	Graphics Interchange Format
GPS	Global Positioning System
JEIDA	Japan Electronic Industries Development Association
JPEG	Joint Photographic Expert Group
IFD	Image File Directory
IQM	Image Quality Metrics
LCD	Liquid Crystal Display
MSE	Mean Square Error
TIFF	Tagged Image File Format
TN	True Negative
TP	True Positive
PRCG	Photo Realistic Computer Graphic
PRNU	Photo Response Non-Uniformity
QF	Quality Factor
RMSRE	Root Mean Square Regression Error
SFFS	Sequential Forward Feature Selection
SIFT	Scale Invariant Features Transform
SPN	Sensor Pattern Noise
SVM	Support Vector Machine

Chapter 1

Introduction

1.1 Motivation

With the rapid development of hardware and software in digital photography, digital still cameras are widely used in the society. Digital images as the outputs of the digital cameras, can record the real happening for supporting evidences and historical events in a wide variety of applications, which include news reporting in journal and magazine, police investigation and law enforcement, medical examinations, consumer photography, etc. The advantages of using digital images in a digital still camera (DSC) system are easy storage, quick transmission and printing, and the possibility to do post-processing.

Meanwhile, due to the advancement of image editing tools, digital images are easily altered with no visual clues left. The credibility of digital images is hence questionable. As examples, two cases of doctored images are shown in Figure 1.1. In Figure 1.1(a), O. J. Simpson murder case is shown. By observing these two images, we find that the image in Time Magazine is darker than the one in Newsweek Magazine. The objective of Time Magazine manipulating the image is that they would like to make it more compelling for the readers. Figure 1.1(b) shows a photo which contains an American air force helicopter and a shark. In fact, this photo is fake, where it is created from two isolated images, i.e. a US air force helicopter on a training exercise

Figure 1.1: Two cases of doctored photos [1]. (a) O.J. Simpson murder case. (b) A US air force helicopter and shark.

in San Francisco, and a shark leaping out of the water off the coast of South Africa. More examples of the forged photos are shown in [1, 5], which are mainly published in the famous newspapers and magazines.

In view of this, image forensics has become an important and urgent research area in order to verify the authenticity and integrity on digital images in recent years. In this thesis, we investigate the underlying correlation between the image and its Exchangeable Image File Format (EXIF) header, and the learned correlation can be used for forensics purposes. EXIF [3, 6] is the DSC image file format standard for storing as the metadata. The EXIF headers provide a lot of available information about digital images. An example of a Joint Photographic Expert Group (JPEG) format image with its EXIF header information is shown using Matlab in Figure 1.2. We are only interested in camera settings under the conditions of surroundings, as shown in Figure 1.2(b). Camera settings from the EXIF headers include f-number, exposure time, ISO speed rating, and white balance. They are commonly recorded by different camera manufacturers across a wide range of models. EXIF headers can help users to better control and understand the corresponding images. These camera settings could affect the image content in many ways. If we can find the relationship between the images and the corresponding EXIF headers, it will be a promising tool for image forensics.

(a)

EXIF Camera Settings	Value
F-Number	5.6
Exposure Time	0.004
ISO Speed Rating	100
White balance	Auto
...	...

(b)

Figure 1.2: An example of a photo with its EXIF header information.

1.2 Overview of Image Forensics

In this section, we review some current image forensics issues and general solutions which are organized as follows. Section 1.2.1 discusses current issues which are closely related with image forensics. Section 1.2.2 briefly introduces the active and the passive forensics, and compares these two categories in image forensics area.

1.2.1 Image Forensics Issues

In recent years, numerous issues related to image forensics are broadly discussed in various phases. We mainly list the forensics issues based on images as follows.

1. Image Manipulation Detection

As one of the important forensics tasks, image manipulation detection has been gained a lot of attention in the recent years, especially when the image editing tools become easily available. The most important objective of image manipulation detection is to solve the problems, i.e. “Is a given image fake?”, as presented in [7–41].

Furthermore, some scientific technologies could discover the processing history,

such as the works in [42–50] exposing the manipulation type on the tampered image. The manipulation types are broadly classified into two categories, i.e. malicious and non-malicious operations. Malicious operations are defined as that the visually acceptable forged photo can manage to deceive the others from the truth while the forged photo is deliberately generated by the attacker. For instance, copy-and-paste operation which pastes the copied interested area into another location in the same image (also called copy-and-move) or in the different image, is detected in [51–68]. Especially, the works in [69–73] focus on locating the forged region. Non-malicious operations affect the perceptual quality of digital images more intensively [74–77]. The works in [38, 78–83] estimated the parameters used on the tampered images. When the given image is manipulated by not only non-malicious operation but also malicious operation, the problem becomes more challengeable, i.e. no visual clues are left. Hence, exploring the evidence in the forgery image is urgently needed.

2. Source Device Identification

As the fast spread and growing popularity of digital cameras, many researchers are particularly interested in addressing the challenges in source camera identification [45, 84–94]. They study source camera identification from which individual camera, what sensor type, model and brand is the device used in capturing a given image to whether a set of the given images can be classified to the correct sources. Majority of the related works identify the sources of cameras. Moreover, the other types of the popular digital source device identification are investigated, such as mobile camera identification as shown in [95, 96], scanner identification as discussed in [97], and printer image identification in [90].

3. Natural Image Identification

By using the modern excellent image display technology, it is highly possible to recapture an image with good quality on the artificial scenery. From another point of view, photo realistic computer graphic (PRCG) image is artificially created by using the computer software. Such good-quality recaptured image and PRCG image have

the possibility to be missed by the current forensics systems. Therefore, the works in [98,99] distinguish the natural images from the recaptured images on liquid crystal display (LCD) screen, or the works in [100–105] differentiate the natural images from the computer graphic images.

4. Temporal Forensics Analysis

In company with today’s highly developed internet, temporal forensics analysis can help the users to better understand the role of the digital images. Specifically, temporal forensics analysis in [106–109] focuses on establishing temporal relationship among a group of images instead of only one single image. Its aim is to construct a graph, which is used to describe image dependency relationship, especially images representing similar or equal content. For instance, the work in [106] ranks a sequence of images according to their capturing time.

5. Steganalysis

Steganography is to embed a secret message into an innocuous looking cover medium, such as image and video, so that stego medium will not reveal the presence of the secret message in the casual inspection. In order to distinguish the stego image from the cover image, a few works on steganalysis in [86, 110–113] have built a universal framework. Majority of these works rely on studying the image statistics, which are relatively consistent across a broad range of images, but are disturbed by the presence of hidden messages. In the future, steganography faces more challenging problem for hidden messages that are able to be transmitted without alarming by steganalysis technologies.

6. Countering Anti-forensics Threat

Although the manipulated images have no visual clues left, some artifacts or inconsistencies are still introduced at the same time. Since this phenomenon has been noticed recently, the experienced attackers may attempt to weaken or conceal the artifacts and inconsistencies in the forgery images. Hence, the works in [114–117]

are proposed in order to counter such anti-forensics threat.

1.2.2 Image Forensics Categories

Various image forensics works [118–121] have been developed in recent years. Generally, existing image forensics works can be categorized as follows:

1. Active image forensics
2. Passive image forensics

Active forensics extracts pre-embedded protective information from the digital images. Digital watermarking [122–124] is a typical type of active approaches for image forensics. Watermarks are inserted into the digital images before the digital images are tampered. Tampering detection is achieved through analyzing the extracted hidden data. Moreover, digital signature also belongs to active forensics category. For instance, the image is authenticated through an encrypted digital signature file in [125]. The first limitation of active forensics is that the pre-embedded protective information has to be inserted into images before tampering, such as watermarks and digital signatures. Otherwise, the pre-embedded protective information cannot verify whether the images are tampered or not. The second limitation is that the integrity of image is corrupted when the pre-embedded protective information is inserted into the image.

In view of the two limitations above on active forensics, passive forensics has been gained more attention by the researchers in the recent years. This thesis focuses on exploring new evidences from the EXIF header for passive forensics. Passive forensics technologies rely on detecting the inconsistent regularities or specific artifacts for manipulation detection. The rationale is that when an image undergoes a type of manipulations, specific artifacts can be introduced and these artifacts can manifest themselves as destroying certain intrinsic image correlations or introducing excessive inconsistencies over some regular structure, which are uncommon for the intact images. So far, various clues are explored for passive forensics analysis by following the

digital camera pipeline. In Chapter 2, we will present the state-of-art methods of passive image forensics in more details.

1.3 Overview of EXIF

In this section, we present an overview of the EXIF header, which contains EXIF history, EXIF structure and EXIF related application. A detailed description of the EXIF header is given as follows.

1.3.1 EXIF History

EXIF is proposed by Japan Electronic Industries Development Association (JEIDA). It is currently supported by Tagged Image File Format (TIFF) format and JPEG format as an international standard in the digital camera system.

Figure 1.3: History of EXIF evolution (courtesy from [2])

Figure 1.3 shows the history of EXIF evolution. EXIF Version 1.0 in [126] was proposed as a standard for storing the metadata by the former JEIDA. On basis of JPEG/TIFF Rev 6.0 structure, tag information structure and basic tag definitions were specified in EXIF Version 1.0. It was established to ensure interchangeability of primary image data. EXIF Version 2.0 in [127] was subsequently improved with sRGB color space compressed thumbnails and audio files in July 1998. EXIF Version 2.1 in [128] was issued by JEIDA in January 1999. It was developed with design rules for the camera file system standard 1.0, which was to enable image files to be exchanged among different recording medias. It was intended for the correct exchange and playback of primary image data. In February 2002, EXIF Version 2.2 in [3] was formalized, which improved compatibility between digital cameras and printers. This simplifies the printing of high-quality images captured by digital cameras. EXIF Version 2.21 in [129] was released in September 2003 as an upgrade version following the design rules for the camera file system Version 2.0. It supports the Adobe RGB color space for the ease of use.

1.3.2 EXIF Structure

An uncompressed EXIF digital image [3] is recorded as a TIFF Revision 6.0, which is shown in Figure 1.4. EXIF is recorded in conformance with TIFF Revision 6.0 [130]. File header is defined in the TIFF standard, with the offset of image file directory (IFD) indicating the start address of the IFD. The initial IFD offset of next image file directory indicates the start address of the first image file directory (thumbnail image). Each of IFD consists of four elements: tag, type, count, and value offset.

A compressed EXIF digital image [3] is recorded as a JPEG file, with application marker segment (APP). Basic structure of compressed EXIF digital image is shown in Figure 1.5. Every JPEG file starts with a start-of-image marker and ends with an end-of-image marker. The EXIF standard uses APP 1 and APP 2 for JPEG segments to store image metadata. If the EXIF metadata is available, it is stored in

Figure 1.4: Basic structure of uncompressed data files (courtesy from [3])

APP 1. This segment follows immediately after the start-of-image marker. If multiple segments of APP2 are present, they start immediately after APP 1. The right side of Figure 1.5 shows a structure of APP 1. EXIF uses the TIFF Revision 6.0 to store data. EXIF provides a lot of available information about the photo.

Figure 1.5: Basic structure of compressed data files (courtesy from [3])

1.3.3 EXIF Related Application

Benefiting from exploring the EXIF header information, EXIF has been adopted in various applications by researchers, such as image retrieval [131–135], simple zoom-lens digital camera calibration [136], and digital watermarking [137, 138]. In [131], Gong *et al.* considered that the scene brightness of photos changes with an event transition of interest. Here, the events can be trips, vocations, weddings, birthday parties, meetings graduation ceremonies etc, which are labeled by users. The scene brightness of photos was extracted from EXIF header for image clustering. In [132], scene modes were utilized for image scene classification. When the users intend to take a photo of the scenery, a scene mode is usually selected, such as firework, portrait, night scene and landscape. Ku *et al.* [132] focused on image scene classification based on firework photos of scene mode and non-firework photos of scene mode. For the

manual settings of the experts, firework photos of scene mode and non-firework photos of scene mode could be differentiated with an accuracy of about 80% based on the scene modes from the EXIF headers. In [133], Jang *et al.* combined the timestamp from the EXIF header and the features from the photos for image clustering. In [134], Matthew *et al.* integrated image content and EXIF for improving classification accuracy. Using the problem of indoor-outdoor classification as an example, EXIF analysis for each class revealed that exposure time, flash use, and subject distance are salient cues. Based on Bayesian network, the accuracy of classification is improved compared with the method based on image content only. In [135], global positioning system (GPS) was utilized for event classification. Though Yuan *et al.* did not specify the GPS information recorded in the EXIF header, GPS can be extracted from EXIF headers of images captured by high-end digital cameras.

Some researchers tried to calibrate the simple zoom-lens digital camera based on EXIF. In [136], Sun *et al.* proposed a simple method to calibrate the intrinsic parameters of zoom-lens digital cameras, where the method combined the classical calibration algorithm of a planar pattern with the EXIF information. The results show that the proposed method can provide accurate intrinsic camera parameters for all the lens settings.

In [137, 138], the EXIF information is considered as watermarks to enhance the image copyright protection. However, their work does not exploit the information provided by EXIF headers for watermarking. Therefore, the contribution of their works is limited.

From these existing works using the EXIF header, we can see that image content is related with the EXIF header in many ways. We consider that it is possible to perform image forensics using the EXIF header information. Hence, we explore the hidden correlation between the image and the corresponding EXIF header in this thesis for forensics purposes.

1.4 Major Contributions

In our work, we explore the consistency of the image with the EXIF header for image forensics analysis. In particular, we focus on modeling the relationship between the image and the corresponding EXIF header. To the best of our knowledge, this is the first work to find the underlying correlation between the image and the corresponding EXIF header for forensics tasks.

Figure 1.6: A suggested framework of modeling various EXIF-Image correlations

In order to better illustrate the contributions, a suggested framework shown in Figure 1.6 is studied for modeling various EXIF-Image correlations, which contains various techniques proposed in different chapters. The proposed framework consists of four major steps: (1) image representation, (2) image feature selection, (3) EXIF representation and (4) modeling the EXIF-Image correlation. In the first step, various image representations are developed in different chapters. For instance, statistical noise features by cooperating standard deviation and mean of noise features are used in Chapters 3-4, and image quality metrics (IQM) features are applied in Chapter 5. Since some factors, such as the image content, could adversely affect the image representation, feature selection is a key issue in the second step. Specifically, Chapter 3 selects significant features by sequential forward feature selection (SFFS) with the criterion of root mean square error (RMSE) in Chapter 3; Chapter 4 uses SFFS in

conjunction with Fisher's Ratio, and Chapter 5 applies eigen feature regularization, respectively. In the third step, various EXIF header information is extracted to represent the EXIF header. Chapter 3 represent the EXIF header by five camera setting parameters. In Chapter 4, three of five camera setting parameters are selected for compact EXIF header representation. Chapter 5 extracts white balance from the the EXIF header. Finally in the fourth step, the suitable correlations between image features and EXIF parameters are modeled. In Chapter 3, a linear regression algorithm is used to correlate five EXIF parameters with the first-order of statistical noise features. In Chapter 4, a non-linear regression algorithm is further developed to estimate the three EXIF parameters by incorporating the second-order of noise features with the first-order of noise features to cater for nonlinearity of the underlying correlation. In Chapter 5, SVM image training and classification method is developed for exploring the correlation between EXIF-white balance and image quality metrics. The details of the contributions are given as follows."

1. Exploring The EXIF Information for Forensics Task

For current image forensics analysis, a new evidence by using the EXIF header information is explored for image forensics analysis. Five extracted EXIF header features are closely related with the image noise, which include aperture, shutter speed, ISO speed rating, brightness value and exposure. By using the linear regression algorithm, each EXIF header feature is computed as a weighted sum of statistical image noise features. The method also utilizes SFFS to select the significant image noise features for better EXIF parameter estimation. A new evidence of the image and the EXIF header integration is proposed, which demonstrates the possibility for developing the EXIF header information for image forensics analysis.

2. Modeling The EXIF-Image Correlation for Manipulation Detection

A generalized model for manipulation detection is proposed by correlating the image statistical noise features with three EXIF header features. By excluding brightness value and exposure, the rest including aperture, shutter speed and ISO speed rating

are used to represent the EXIF header. The reason to exclude brightness value and exposure is that they would not help much for establishing the EXIF-Image model due to their linear relationship. By further investigating the correlation between statistical noise features and three EXIF header features, the non-linear regression algorithm is employed to establish the EXIF-image model. Specifically, when using the statistical noise features to estimate each EXIF header feature in the authentic image, smaller numerical difference is generated compared with the relatively larger numerical difference in the manipulated image. By using the numerical difference as a manipulation indicator, we can detect common brightness and contrast adjustment. Based on cameras of different brands, our manipulation detection is also demonstrated to work well in a blind mode, where the camera brand and model source is unavailable. Several detection examples suggest that our model can be applied in detecting real-world forgeries.

3. Recognizing The EXIF-White Balance Value for Forensics Analysis

We propose an image tampering detection approach by exploiting EXIF-white balance information which is ignored by previous approaches. For each level of white balance in the EXIF header, IQM features between each two combination of one original image and its twelve re-balanced images are first extracted and then the compact set of image eigen features are selected for recognizing different EXIF-white balance levels by using SVM classifier. Image manipulation like copy-and-paste operation can affect these image eigen features and lead to a wrong white balance level. By using the EXIF-white balance parameter as a manipulator indicator, the proposed approach has the ability to distinguish different levels of white balance applicable for image tampering detection. Our proposed approach can confidently detect complex image tampering, i.e. copy-and-paste followed by the high compression.

1.5 Organization of This Thesis

This thesis mainly focuses on exploiting the EXIF header information for image manipulation detection. The thesis is organized as follows.

- In Chapter 1, image forensics analysis is briefly introduced, which contains the motivation, the overview of current forensics issues and methods, the overview of the EXIF header, and the major contributions of this thesis.
- In Chapter 2, a background and literature review for passive forensics is discussed. The evidences used in the state-of-the-art passive forensics systems are reviewed by following the pipeline of the DSC system, which include the scene regularity, optical regularities in the optical lens, sensor imperfections, processing regularities in the digital processing unit, the generic statistical regularities, and EXIF-based prior works.
- In Chapter 3, a novel evidence for forensics task is explored from the EXIF header. This chapter proposes a method by modeling the EXIF-Image correlation using the linear regression algorithm, where the image is represented by statistical image noise features and the EXIF header is represented by aperture, shutter speed, ISO speed rating, brightness value and exposure respectively. The experimental results demonstrate the possibility of using the EXIF header information for image forensics analysis.
- In Chapter 4, a generalized EXIF-Image model is further established based on the non-linear regression algorithm. Specifically, the statistical noise features including mean and standard deviation of noise features are correlated with aperture, shutter speed and ISO speed rating in the EXIF header. By applying the EXIF-Image model for detecting different brightness and contrast adjustments, the proposed method performs well, even on the real-world forgery examples.
- In Chapter 5, EXIF-white balance is developed for image manipulation detection, where white balance levels in the EXIF header are recognized for forensics

analysis. Based on the correlation between the EXIF-white balance and the image, IQM features are used to represent the given image. The SVM is used as the classifier.

- In Chapter 6, a conclusion of the thesis is given and several possible directions for future research are discussed.

Chapter 2

Background and Literature Review

In this chapter, we review the background and literatures related to current image forensics technologies. As the whole thesis is based on passive forensics structure, this chapter will focus on current passive forensics technologies. Firstly, the processing pipeline of the digital camera system is introduced for preparing the basic knowledge of passive forensics. After understanding more about the digital still camera (DSC) system, five different types of evidences for current passive forensics are analyzed according to the camera pipeline, and further compared in the summary of this chapter.

2.1 Digital Still Camera System

In order to better understand image forensics analysis, we first introduce the basic knowledge of the image generation processes inside the DSC system [139] as shown in Figure 2.1.

Firstly, the light photons from the actual scenery enter into the digital camera. When the light photons arrive at the optical lens system, several optical filters including the anti-aliasing filters and infrared rejection filters are used to filter the light photons. In the following step, the light photons pass through the color filter array

Figure 2.1: The pipeline of the DSC system

(CFA). As each tiny color filter is placed on top of one sensor, a specific color at every pixel in the whole image is measured. So far, charge-coupled device (CCD) and Complementary Metal Oxide Semiconductor (CMOS) sensors are two types of the most commonly used sensors to sense the luminance. After each sensor gets the color information, CFA interpolation is applied to reconstruct the three-colored image, where the procedure of interpolating the missing color samples is also called demosaicing. Finally, the reconstructed image will go through a series of software processes, such as gamma correction, white balance, lossy JPEG compression, so that an image is generated as the digital camera output.

2.2 Current Passive Forensics Evidences

After obtaining the knowledge of the commercial cameras sold today, various evidences adopted by passive forensics technologies are investigated. Though many tampering operations produce tampered images without any visual clues of tampering, it is still observed that the distribution of the artifacts from some tampered images is not fairly uniform compared with that of the artifacts from the genuine images. The existing works of passive image forensics detect inconsistencies of certain image regularities in the origins of different parts of digital camera system instead of hiding additional information in the image. According to sources of forensics features, we can divide the forensics clues into five categories including the scene regularities, the

optical component features, the sensor defect patterns, the digital processing regularities and some generic statistical features. More details about these five categories are discussed as follows.

2.2.1 Scenery Regularities

When the scenery is captured for an image generation, the geometry regularities in the authentic images are used as the clues for exposing the forgery images. The theoretical basis is the presence of inconsistent geometry regularities in forgery images, such as lighting condition, shadow, planar homography and circles in geometric distortion.

Lighting Condition

Johnson *et al.* [16] proposed a forgery detection method by detecting lighting inconsistency, as the lighting conditions in the composite image is difficult to keep consistent. In particular, the two-dimensional surface normals at the occluding object boundary are used to approximate two components of light source direction for detecting lighting inconsistency. In [17], a three-dimensional light source direction is developed for exposing the tampered photo, where the proposed algorithm relies on analyzing a model of specular highlights on human eyes. The complex lighting environments are investigated for identifying the doctored image in [18], which models the complex lighting conditions as the linear sum of spherical harmonic functions.

Shadow

As a normal phenomena in the real world, shadows reveal a certain amount of visual cues, e.g. depth, shape, etc. In [19], Zhang *et al.* extracted the shadow matte value for exposing the tampered images by computing the color intensity medians of two regions laid in and out sides of the shadows and comparing the ratio between them. When the constraint that the surface receives the flat and not textured shadow is satisfied, this proposed method performs well. Since the shadows are not always

projected without textured surface in reality, Liu *et al.* [62] developed a framework for identifying the tampered images by detecting photometric consistency of illumination in shadows. Specifically, estimating the shadow matte value from a single view of a target scene is used for image digital forgery detection. The two works in [19,62], solve the forensics problem when a unique object-to-shadow pairing was available. In [20], Kakar *et al.* proposed a two-stage shadow detection method for authenticating the captured time of the image based on the geolocation information. Furthermore, Kee *et al.* [21] exploited a broad range of ambiguous cast and attached shadows on the projected location of a point light source. By formulating the consistency of the shadows in a linear programming problem, a failure to find the solution indicates the tampered image.

Text

In [22], Conotter *et al.* proposed a new forensics approach to detect the manipulated text. The idea is that the typed text on a sign or billboard obeys the rules of perspective projection. When the text in an image is manipulated, the projection of text on a planar surface will be deviated from the estimated model in the authentic image. A set of experiments show that the proposed method has the capability to detect manipulated text whether the font style of the text is known or unknown.

Geometric Distortion

Zhang *et al.* [59] proposed an approach for first roughly locating the fake object based on the planar homography and then segmenting it using graph cut with online feature or parameter selection. The rationale is to detect inconsistencies of geometry distortions, where the distortions of shapes and positions in one image are related with another image monitoring the same scene. Due to the planar homography constraint, the proposed method only works in the following cases: (1) a single image with duplications, e.g. copying and pasting a region to a different position; (2) image pairs captured of the same scene but with different setups, e.g. famous landmarks photographed by various tourists over the years.

Johnson *et al.* [56] considered two eyes of a person in the image as two circles. By estimating the principal points of the camera from two eyes with the prior knowledge of the focal length required, inconsistencies in principal points are adopted to detect image composite. The primary limitation is that the proposed method is difficult to perform on the low resolution images. In order to solve the forgery detection problem on the low resolution images, Kee *et al.* [23] applied a set of co-planar facial features, including the corners of the eyes, the base of the nose and the chin, to detect the composite photos of famous people. However, this method requires an image containing at least a reference person and a testing person both of which directly face the camera. Although the required case is not practical, it is useful when analyzing composite photos of famous people, for which a reference photo is easily obtained from an on-line image search, or for any person or object whose reference photo is available. In [24,64], Zhu *et al.* first estimated the focal length based on the equality of the sizes of two coplanar circles for detecting inconsistencies in the angles among the normal vectors. Furthermore, tampering the image with a single circle is also studied by warping the circle for metric measurement, where a single circle is either with its discriminable center or with geometric constraints for camera calibration.

Zhang *et al.* [57] detected image composites on image pairs based on the two-view geometrical constraints. The proposed method is efficient to detect the forgery image, when the fake photos are generated from two images captured of the same scene.

2.2.2 Optical Regularities in Optical Lens

When the light photons pass through the optical lens system, lens produces various types of aberrations in images. Hence, detecting the consistencies of optical regularities is one of good ways for forensics analysis, which includes chromatic aberration and lens radial distortion.

Chromatic Aberration

In an optical system, chromatic aberration is one of the most popular evidences for forensics analysis. Chromatic aberration is caused by the failure of the lens to perfectly focus light of all wavelengths, which includes longitudinal aberration and lateral aberration. Lateral aberration happens by a spatial displacement in the locations where light of different wavelengths reaches the sensor. In [25], Johnson *et al.* detected the inconsistency of lateral chromatic aberration over an image as an evidence of image tampering. Lateral chromatic aberration was modeled as the expansion or contraction of the color channels with respect to one another using the low parameter model. If the image was tampered, the chromatic aberration can become inconsistent over the image. The weakness is that chromatic aberration cannot be estimated in the block with little or no spatial information, such as uniform regions of the sky.

Instead of approximating a specific aberration such as lateral chromatic aberration in [25], or modeling the complex intermixing of various aberrations in the image, Yerushalmy *et al.* [26] proposed a method to learn the specific local characteristics to represent the aberration cues. Since these aberration cues are abundant in the image, the proposed method has the ability to identify the authenticity of the given image, detect the cropped image followed by restoring the original size and shape, and determine the forgery image by passing through the copy-and-paste operation.

Lens Radial Distortion

In [27], Choi *et al.* exploited the lens footprints left as the forensics evidence, i.e. the lens radial distortions in the images for source camera identification. By applying the learned classifier on lens radial distortion, the encouraging results obtained prove that lens radial distortion is one of the useful forensics evidences. It is noting that the proposed method works when the images are taken by digital single lens reflex (DSLR) cameras with prime lens (fixed focal length lens) or the prior knowledge of the images taken with zoom lens but without manual zooming is required. While images from a specific camera are taken by zoom lens with different manual zooming

settings, the measured lens distortion parameter spanning over a large range results in the decreased accuracy of the proposed method.

2.2.3 Sensor Imperfections

Several types of sensor imperfections evidences are discussed for forensics proposes, which include sensor noise pattern, dust pattern and camera response function.

Sensor Noise Pattern

In the sensor manufacturing process, photo response non-uniformity (PRNU) which is caused by different sensitivity of pixels to light, is the dominant pattern noise. In [28], the sensor pattern noise was used for image tampering detection. If the image was tampered, the sensor pattern noise was not presented. The noise patterns obtained from various regions were firstly correlated with the corresponding regions in the camera's reference pattern and then a decision was made based on comparisons of correlation results of regions of interest with those of other regions. Chen *et al.* further developed the PRNU sensor noise estimation model for camera identification and forgery detection in [45]. Due to the limitation that the sensor pattern noise (SPN) extracted from images can be severely contaminated by details from scenes, Li *et al.* in [29] enhanced sensor noise pattern for improving the accuracy of source camera identification. Theoretically, the hypothesis used in [29] is that the strong signal component in an SPN results in less trustworthy and should be attenuated. The proposed method is capable to counter the influence of details from SPNs for identifying source cameras. In [97], Gou *et al.* extended statistical noise features to identify the sources of scanner images. Furthermore, the proposed method is used to detect the manipulated scanner images that have gone through different types of operations, which include additive noise, average filtering, median filtering, sharpening, contract enhancement, gamma correction, sharpening, rotation, resizing, and JPEG compression.

Dust Pattern

Dirik *et al.* [30, 87] exploited dust spots or blemishes in DSLR camera images for source camera identification. As the sensor dust spots are considered as the artifacts on the captured images, a Gaussian intensity loss model is used to learn dust spots patterns for the given camera. The proposed approach demonstrates that the artifacts caused by the appearance of dust spots or blemishes can be utilized as a fingerprint of the camera, especially when the smaller aperture values make sensor dust more visible. However, the proposed method has less ability to detect dust spots in the very complex regions and low f-number. Furthermore, traces of dust, dirt, and scratches over scanner platen on scanned images are applied for the individual source scanner identification in [31].

Camera Response Function

Lin *et al.* [32] developed a method for detecting the splicing operation on the high-contrast images with many textureless edges. Specifically, anomalies of the Camera Response Function (CRF) in suspicious boundaries are detected, where suspicious boundaries are manually located. In order to estimate CRF better, Hsu *et al.* [33, 55] proposed a fully automatic method for forgery detection. Moreover, instead of simply estimating the anomalies of CRF in [32], the proposed method in [33, 55] benefits from CRF-based cross fitting and local image features. The experimental results show that CRF is a promising tool for image splicing detection. Ng *et al.* [34, 35] exploited the CRF signature from a single image based on an edge-profile method, without learning data required. The experimental results demonstrate that CRF is a promising tool for image forensics tasks in many ways, which include source camera identification, tampering detection, etc. However, the primary drawbacks of the proposed method are straight and wide edges required for reliably extracting the edge profiles, and accurate derivative estimation.

2.2.4 Processing Regularities in The Digital Processing Unit

Many software processes are utilized for image generation. Here, we discuss the commonly used software processing for image forensics, which include demosaicing, JPEG compression, resampling and white balance.

Demosaicing

In the DSC system, the types of CFA and the demosaicing algorithms are different among different digital camera brands and models. The most commonly used filter is Bayesian filter which captures green, red and blue light. The green light is sampled two times of the red or blue light. Demosaicing is a form of interpolation, which can introduce correlations between the pixels of an image. If the image is tampered, the distribution of demosaiced features will not be fairly uniform over the whole image. Hence, detection and localization of image tampering can be performed based on the inconsistency of the demosaiced features in the color filter array. In [42], Popescu *et al.* estimated the linear interpolation filter coefficients based on the expectation/maximization algorithm with the different CFA interpolation algorithms. Based on the presence of CFA interpolation, Popescu *et al.* detected the image tampering. In [43], a non-intrusive component analysis framework is developed by estimating the potential CFA pattern and color interpolation coefficients. In particular, the extrinsic image manipulation is computed as a linear process of time invariant filtering, and the estimated filter parameters through the recursive deconvolution technique are applied to expose different types of image tampering operations. In [93], Cao *et al.* estimated demosaicing weights features for image manipulation detection. The experimental results show that good performance is achieved among multiple images from different mobile devices. As discussed in [42, 43, 93], it is relatively easy to discriminate camera sources among different camera brands, but difficult to distinguish the cameras among similar camera models. By considering this problem, the compact templates models are derived in order to identify similar DSLR cameras, in [36]. The proposed method in [95] developed demosaicing features for determining the integrity of mobile

images.

JPEG compression

As we know, JPEG is the most popular image format in today's commercial cameras. When a JPEG image is tampered, the image is first decoded into spatial domain, and regions of interest in the image are modified. Finally, re-compression is performed for generating a JPEG image. Hence, re-compressing JPEG artifacts are detected for image forensics analysis. For instance, He *et al.* [44] developed a generalized model to detect doctored JPEG images and further located the doctored parts, by evaluating the double quantization effect hidden among the discrete cosine transform coefficients. Ye *et al.* [37] proposed an approach for tampering detection by estimating JPEG artifacts in the local compression blocks. Farid in [46] detected the composite image generated by two or more different original images with different JPEG compression quality. Qu *et al.* [38] detected re-compressed images with block shifting in order to counter the operation of cropping the JPEG images with several rows or columns before re-compression.

Resampling

Popescu *et al.* in [74] proposed a method to detect re-sampling operation, where it is highly possible to happen on the fake images. In particular, specific periodic correlations between the image pixels are detected in any region of the given image. However, the proposed method only works on uncompressed TIFF images, JPEG and Graphics Interchange Format (GIF) images with minimal compression.

White balance

Deng *et al.* [140] used white balance to identify the camera sources. The rationale is that a digital image would not change much compared with the re-balanced image if the same auto white balance algorithm is applied twice. Although the specific white balance algorithm used inside the camera is unknown, the majority of the cameras are designed for adjusting different lighting conditions by applying auto white balance

technologies, and there exists some discrimination among different digital cameras. A set of experimental results show that the proposed method is effective to identify cameras from different brands and models.

2.2.5 Generic Statistical Regularities

Some generic statistical regularities are exploited for forensics analysis. For instance, bicoherence, image histogram in spatial domain, and the statistical regularities in frequency domain.

Statistical Regularities in Spatial Domain

Ng *et al.* [39] detected image splicing by bicoherence features in the blind model. Cao *et al.* [77] proposed a forensics approach by detecting statistical abnormality on image grayscale histograms for identifying and reconstructing gamma correction operations in digital images. The proposed approach has ability to determine the manipulated image which is subject to global or local gamma correction.

Intrinsic Fingerprint in Frequency Domain

Stamm *et al.* [40] proposed a method for manipulation detection by analyzing the intrinsic fingerprint in the frequency domain. Specifically, the proposed method has ability to detect global and local contrast enhancement, histogram equalization, and additive noise in a previously JPEG-compressed image.

2.2.6 EXIF-based Prior Works

Since various variable information about the JPEG photo is recorded as metadata, EXIF has gained more attention by image forensics in the recent years. Several works have appeared which utilize the EXIF header parameters for the forensics analysis.

EXIF Parameter

Among the existing tampering forensics works, Johnson and Farid [56] extracted the focal length parameter from the EXIF header to estimate the principal point location in the image of eyes for detecting photo composite of people.

EXIF Standard Format

Kee *et al.* in [41] extracted a 576-dimensional camera signature including 8 extracted EXIF values for deterministic image authentication. These eight features characterize the EXIF header format, which is supposedly common for cameras of the same model. In the scenario of image authentication, for example, when the camera make/model name is changed in an attempt to conceal the camera source, the extracted signature would become inconsistent with the known authentic camera signature. Although image manipulation often causes detectable header changes, we note that Kee's method does not directly authenticate the image content. Hence, it would not work in the scenario that a forger deliberately keeps the header intact after manipulating the image content.

2.3 Comparison of Different Evidences

Different types of forensics evidences have been exploited in recent years. They mainly focus on manipulation detection and source device identification as shown in Table 2.1. According to the digital camera pipeline, we will compare different types of forensics evidences in four major phases. These four major phases include six types of forensics evidences, each type of evidences addressing to the corresponding forensics issues, each evidence performing on the formats and the scenery content of images.

- **Scenery Regularities** including lighting condition in [16–18], shadow in [19, 21, 62], text in [22] and geometric distortion in [23, 24, 56, 57, 59, 64] are used to detect the composite image in JPEG format. The primary drawback of the works in [16–19, 21–24, 56, 57, 59, 62, 64] by using scenery regularity as the

Table 2.1: Comparison of Different Evidences

Camera System	Evidences	Forensics Issues			Image Format	Image Content
		Manipulation detection	Source identification			
Scene Regularities	Lighting Condition [16–18]	✓	Photo composite	×	JPEG	Special
	Shadow [19–21, 62] Text [22] Geometric Distortion [23, 24, 56, 57, 59, 64]					
Optical Regularities	Chromatic Aberration [25, 26]	✓	Copy-and-move, Copy-and-paste, Cropping	×	JPEG	Normal
	Lens Radial Distortion [27]	×	Nil	✓		
Sensor Imperfections	Sensor Noise Pattern [28, 29, 45, 97]		Copy-and-move, Copy-and-paste Additive noise Average/Median filtering Contract enhancement Gamma correction Rotation, Resizing JPEG compression Sharpening	✓	JPEG, TIFF	Normal
		×	Nil	✓	JPEG	
		✓	Image splicing	✓		
		✓	Copy-and-paste	✓		
Processing Regularities	JPEG compression [37, 38, 44, 46]	✓	Inpainting, Matting, Image splicing, JPEG compression	×	JPEG, TIFF	Normal
	Resampling [74]	✓	Resampling	×	JPEG, TIFF, GIF	
	White balance [140]	×	Nil	✓	JPEG	
	Bicoherence [39]		Image splicing			
Statistical Regularities	Grayscale histogram [77]		Gamma correction			
	Intrinsic Fingerprint in Frequency Domain [40]	✓	Contrast enhancement Histogram equalization Additive noise	×	JPEG	Normal
EXIF-based	Focal length [56]	✓	Copy-and-move	×	JPEG	Normal
	EXIF standard format [41]		Nil			

evidence is that the image content is captured of some special scenery, such as shadow, circles, etc.

- **Optical Regularities** including chromatic aberration in [25,26] and lens radial distortion in [27], are exploited for tampering detection, where the tampered images in JPEG format are subject to copy-and-move, copy-and-paste, cropping and contain various normal sceneries.
- **Sensor Imperfections** including sensor noise pattern in [28, 29, 45, 97], dust pattern in [30, 31, 87], and camera response function in [32–35, 55], are applied to identify the sources of the camera JPEG images. Among all the evidences of sensor imperfections, sensor noise pattern and dust pattern are extended to scanner identification. Furthermore, sensor noise pattern is used to detect the manipulated image, which is subject to a wide range of operations. Camera response function is utilized for image splicing detection. All the images for extracting sensor imperfections are taken of various normal sceneries.
- **Processing Regularities** including demosaicing in [36, 42, 43, 93, 95], JPEG compression in [37, 38, 44, 46], resampling in [74], and white balance in [140], are exploited for forensics purposes. Demosaicing, JPEG compression and resampling have the ability to distinguish a manipulated image in multiple image formats, e.g. resampling image in JPEG, TIFF and GIF formats. Demosaicing is used for camera and scanner identification and white balance is used for source camera identification.
- **Generic Statistical Regularities** including bicoherence in [39], grayscale histogram in [77], and intrinsic fingerprint in frequency domain in [40], are used for manipulation detection. Specifically, the manipulated images in JPEG format are subject to the operations of copy-and-paste, gamma correction, contrast enhancement.
- **EXIF-based** including focal length in [56] and EXIF standard format in [41] are used to facilitate the forensics analysis and the roles of EXIF parameters play minimal. In particular, focal length in [56] is required as the prior knowledge for copy-and-move detection. EXIF structure in [41] is applied for image

authentication, which did not involve any content tampering.

2.4 Summary

In this chapter, the existing forensics evidences are roughly categorized into 6 different classes following the camera pipeline and compared in different phases. By investigating current prior works of passive forensics, we find that exploring the new evidences from the EXIF header is a promising way for image forensics analysis.

Chapter 3

Exploring The Novel Evidence for Image Forensics Analysis

EXIF is a metadata header containing shot-related camera settings such as aperture, exposure time, ISO speed etc. These settings can affect the photo content in many ways. In this chapter, we explore the novel evidence from the EXIF header for image forensics analysis. To the best of our knowledge, this is the first forensics work that explores the potential EXIF-Image correlation in the linear regression algorithm for image manipulation detection. The proposed framework and procedures are explained in details. The experimental results show the effectiveness of the proposed method in detecting the presence of common image brightness and contrast adjustment in three different camera brands.

3.1 Introduction

In order to explore the novel evidence for image forensics analysis, camera settings in the EXIF headers are correlated with image statistical noise features. Different from prior forensics evidences, the EXIF-Image correlation exploits the rich EXIF header information about the images.

Moreover, the photon transfer curve in [141,142] shows that the standard deviation

of total sensor noise is correlated with digital camera signal intensity (DCSI), i.e. the amount of effective light impinging onto an image sensor during the shutter-opening period. Since DCSI is closely associated with some EXIF settings, e.g. aperture and exposure time, and the standard deviation of sensor noise can be evaluated from the photo, potentially this correlation can be modeled and explored as EXIF-Image correlation for forensics purposes. Inspired by this finding, we investigate and learn the correlation between several selected EXIF features and image statistical noise features as several sets of regression weights. When applied to detect image manipulation, the learned EXIF-Image correlation is demonstrated to be effective in detecting the presence of common image brightness and contrast adjustment.

The rest of the chapter is organized as follows. Section 3.2 investigates the background knowledge for modeling the correlation between the image statistical noise features and the camera setting in the EXIF header. In Section 3.3, we model the correlation between an image and its EXIF header. The learned correlation is used to detect image manipulation in Section 3.4. Section 3.5 concludes our work.

3.2 Image Noise Associated with Camera Settings in EXIF

In this section, we will study some common camera settings [143] in the EXIF headers associated with image noise features.

3.2.1 Image Visual Noise Pattern

By considering the EXIF rich information in diverse camera brands and models, camera settings such as f-number (aperture), exposure time and ISO speed rating can affect the photo in numerous aspects. As an example, Figure 3.1(b-d) show three photos captured of the same scenery in Figure 3.1(a) with different ISO speed ratings and other settings kept as constant. We observe that brighter image and more visual

noise are associated with higher ISO speed rating. The visual investigation in Figure 3.1, suggests a potential relationship between the image and its camera settings in the EXIF header.

Figure 3.1: Visual noise comparison for images captured of the same scenery by a Canon 550D camera with different ISO speed ratings. (a) Ground-truth scenery. Captured images (b) with ISO=800; (c) with ISO=3200 and (d) with ISO=12800. f-number and exposure time are fixed at 4.5 and $\frac{1}{60}$ second.

3.2.2 Photon Transfer Curve

When the photo is captured by the digital camera from the real world, the key process [142] is that light signals are converted into digital signals. As shown in Figure 3.2, the light reflected by the subject passes through a set of compound lens first. According to the amount of light measured by light metering, the aperture size and the opening time of the shutter are determined by the camera. The light falling on the image sensors is converted to electric signals by the image sensor array. By

considering CCD in our case, the digital number of the output signal represents the average signal for a group of pixels on the fixed size of CCD.

Figure 3.2: Process of converting light signals into digital signals in a DSC system.

Figure 3.3: Photon transfer curve.

Furthermore, the photon transfer curve in [141,142] shows that there exists a relationship between image statistical noise features and EXIF header features. In Figure 3.3, the x -axis of the photon transfer curve represents DCSI under the conditions of surroundings in the given time period, and the y -axis of the photon transfer curve represents the standard deviation of total noise of the image sensor output. These two quantities have a linear-alike relationship in the large portion of log-scale plots. By studying the photon transfer curve, we find that image statistical noise features can be used as an approximation for the total noise of the image sensor output and

DCSI is determined by camera settings in the EXIF header. Below, we describe the effect of three camera setting parameters on the images taken of the same scene.

3.2.3 Camera Settings from The EXIF Header

The EXIF header information may be different in various camera models and sources according to the needs of different camera manufacturers. However, the basic EXIF header information can be stored in majority of cameras, such as camera settings. Here, we investigate basic camera settings in the EXIF header, which include f-number, exposure time, ISO speed rating.

Exposure Time

Figure 3.4: Images of the same scene captured with exposure time decreased by one full *stop* and other settings unchanged. Top row from left to right: exposure time = 15, 8, 4. The middle row from left to right: exposure time = 2, 1, $\frac{1}{2}$. Bottom row from left to right: exposure time = $\frac{1}{4}$, $\frac{1}{8}$, $\frac{1}{15}$.

Exposure time is the duration that the shutter is held open to allow lights to enter the camera. If the exposure time is longer, more lights will reach the image sensor and vice versa. Figure 3.4 shows that the images of the same scene are captured with decreasing exposure time, each time by one full *stop*. As we can see, the shorter the exposure time, the darker the image obtained.

Figure 3.5: A small f-number as shown in top row and a big f-number as shown in the bottom row (courtesy from [4])

F-number

F-number is related with the diameter of the aperture in terms of the effective focal length of the lens, as shown in Figure 3.5. A bigger f-number corresponds to a smaller diameter of the aperture and less light per unit area reaching the image sensor.

Figure 3.6 shows the images of the same scene captured by increasing f-number at a unit of full *stop*. The change of one full *stop* physically means that the light arriving at the image sensor becomes halved or doubled. The smaller the f-number, the more the aggregate amount of light arrives. Hence, the brighter image is obtained.

Figure 3.6: Images of the same scene captured with f-number changed by one full *stop* and other settings unchanged. Top row from left to right: f-number = 2.8, 4.0, 5.6. Bottom row from left to right: f-number = 8.0, 11, 16.

ISO Speed Rating

ISO speed rating tells the sensitivity of the image sensor to the lights. The higher ISO speed rating, the more lights fall on the image sensor. Figure 3.7 shows the images of the same scene captured with ISO speed rating increased by one full *stop*. The larger the ISO speed rating, the brighter the image obtained.

Figure 3.7: Images of the same scene captured with ISO speed rating increased by one full *stop* and other settings unchanged. The row from left to right: ISO = 100, 200, 400.

3.3 Proposed Method

Figure 3.8 is the block diagram for modeling the EXIF-Image correlation in the linear regression algorithm. In the blocks labeled “Extraction of Image Statistical Noise Features” and “Extraction of EXIF Header Features”, the procedures for extracting statistical noise features from the images and for extracting EXIF header features from the image headers are shown, respectively. The correlation between image noise features and EXIF header features is learned in the block labeled “Modeling The EXIF-Image Correlation in Linear Regression”. The detailed procedures are explained in the following section.

Figure 3.8: Modeling the correlation between images and each EXIF header feature in the linear regression

3.3.1 Extraction of Image Noise Features

We statistically extract a set of image noise features based on four types of denoising filters. Since the noise estimation can be adversely affected by the heterogeneous image content, especially in the sharp transitional area, we compute our noise features based on the non-sharp image area.

Given an $M \times N$ color image $\mathbf{A} = \{\mathbf{A}^{(c)}\}$, where $c \in \{red, green, blue\}$ denotes

the index of a color channel and $\mathbf{A}^{(c)} = \begin{bmatrix} A^{(c)}(1, 1) & \cdots & A^{(c)}(1, N) \\ \vdots & \ddots & \vdots \\ A^{(c)}(M, 1) & \cdots & A^{(c)}(M, N) \end{bmatrix}$, we first

estimate the sharp area map using its grayscale image $\mathbf{L}$ [144], which can be computed using

$$\mathbf{L} = 0.2989\mathbf{A}^{(r)} + 0.5870\mathbf{A}^{(g)} + 0.1140\mathbf{A}^{(b)} \quad (3.1)$$

(a)

(b)

Figure 3.9: An example of the sharp area in the histogram distribution of the edge magnitude signal of the image. (a) A Photo (b) The sharp area in the histogram distribution of the edge magnitude signal regarding the image (a)

(a)

(b)

Figure 3.10: An example of the sharp edge area before and after dilating the grayscale image. (a) Before dilation (b) After dilation

The sharpness residual image is then estimated as

$$\mathbf{G} = |\mathbf{L} - \mathbf{L} * \mathbf{O}| \quad (3.2)$$

where $\mathbf{O}$ represents a 3×3 Gaussian smoothing filter and “*” denotes convolution. We plot the normalized histogram distribution of the sharpness residuals $\mathbf{G} = \{G(m, n) | m = 1, \dots, M, n = 1, \dots, N\}$ in Figure 3.9(b). We then define whether a pixel location (m, n) is in the sharp area using

$$B(m, n) = \begin{cases} 1 & \text{if } G(m, n) \geq r \\ 0 & \text{if } G(m, n) < r \end{cases} \quad (3.3)$$

where $B(m, n) = 1$ indicates that the location (m, n) is in the sharp area and r is a threshold. We choose r empirically to be the value corresponding to 0.9 of the cumulative distribution of the sharpness residuals. This means the top 10% pixel locations with the larger sharpness residuals are classified as the sharp area and the remaining as the non-sharp area. To ensure that these sharp locations would not affect our noise estimation, we further expand the sharp area $\mathbf{B}$ through dilation using

$$\mathbf{K} = \mathbf{B} \oplus \mathbf{V} \quad (3.4)$$

$$\text{where } \mathbf{B} = \begin{bmatrix} B(1, 1) & \cdots & B(1, N) \\ \vdots & \ddots & \vdots \\ B(M, 1) & \cdots & B(M, N) \end{bmatrix}, \quad \mathbf{V} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \text{ is a structure element}$$

$$\text{and } \mathbf{K} = \begin{bmatrix} K(1, 1) & \cdots & K(1, N) \\ \vdots & \ddots & \vdots \\ K(M, 1) & \cdots & K(M, N) \end{bmatrix} \text{ is the expanded sharp area map with one}$$

example shown in Figure 3.10(b).

With the map $\mathbf{K}$ known, we then compute the statistical noise features within the non-sharp area. Knowing that different denoising filters are effective in removing different types of image noises [97], we choose a set of denoising filters to extract the noise features as follows.

- Averaging filter of 3×3 pixels designed for the removal of the high-frequency noise
- Gaussian filter of 3×3 pixels with mean 0 and standard deviation 0.5 designed for the removal of the high-frequency noise
- Median filter of 3×3 pixels designed for the removal of salt and pepper noise
- Wiener filter of 3×3 pixels designed to remove the noise associated with the local pixels

For each combination of color channel $\mathbf{A}^{(c)}$ and denoising filter $\mathbf{H}^{(d)}$, $d = 1, \dots, 4$, we compute the mean μ_{cd} and standard deviation σ_{cd} of the log-scale noise residuals as our noise features using

$$\begin{aligned}\mu_{cd} &= \frac{1}{R} \sum_{\substack{K(m,n)=0 \\ f(m,n)>0}} \log_2(f(m,n)) \\ \sigma_{cd} &= \left(\frac{1}{R} \sum_{\substack{K(m,n)=0 \\ f(m,n)>0}} (\log_2(f(m,n)) - \mu_{cd})^2 \right)^{\frac{1}{2}}\end{aligned}\tag{3.5}$$

$$\text{where } \mathbf{D}^{(cd)} = \mathbf{A}^{(c)} * \mathbf{H}^{(d)} = \begin{bmatrix} D^{(cd)}(1,1) & \dots & D^{(cd)}(1,N) \\ \vdots & \ddots & \vdots \\ D^{(cd)}(M,1) & \dots & D^{(cd)}(M,N) \end{bmatrix}, \quad f(m,n) =$$

$|A^{(c)}(m,n) - D^{(cd)}(m,n)|$, and R is the total number of non-sharp locations. Note that inspired by the log-scale plot of the photon transfer curve in Figure 3.3, statistical noise features are computed in the log-scale. Different from the noise features proposed for scanner identification [97], our noise features are computed in the non-sharp area to suppress the adverse effect caused by heterogeneous image content. This improves our estimation of the EXIF-Image correlation.

We compute a 24 dimensional feature vector from each image $\mathbf{A}$ for a total of $3 \times 4 = 12$ combinations of color channels and denoising filters.

3.3.2 Extraction of EXIF Header Features

Camera settings expressed in the log scale are used to represent the EXIF header. The EXIF header features are extracted from the EXIF header for a given training image, as given in [145].

(1) Aperture Value

$$y_1 = \log_2(F^2) \quad (3.6)$$

where F is the f-number. The larger the aperture value, y_1 , the less the amount of light per unit area reaches the image sensors and vice versa.

(2) Shutter Speed Value

$$y_2 = \log_2\left(\frac{1}{t}\right) \quad (3.7)$$

where t is the exposure time. The larger the shutter speed value, y_2 , the less the amount of light reaches the image sensors and vice versa.

(3) ISO Speed Rating Value

$$y_3 = \log_2\left(\frac{I}{3.125}\right) \quad (3.8)$$

where I is the ISO speed rating. The larger the ISO speed rating value, y_3 , the more the amount of light falls on the image sensors and vice versa.

(4) Brightness Value

$$y_4 = y_1 + y_2 - y_3 \quad (3.9)$$

It is the total amount of the light that is reflected from the scenes. The larger the brightness value, the more light reflected from the scenes. Brightness value can be extracted from the EXIF header directly. However, there are only some high-end digital cameras which can record it. Another possible way is to get

it indirectly using Eq. (3.9), which is the one we choose to get the brightness value.

(5) Exposure Value

$$y_5 = y_1 + y_2 \quad (3.10)$$

It refers to camera exposure. It is a set of the combinations of aperture value, and shutter speed value. The larger the exposure value, the less the amount of light falls on the image sensors.

The above EXIF header features share a common unit of *stop*, where the change in one *stop* indicates that the amount of light falling on the digital sensor is doubled or halved. The EXIF header feature vector is represented as $[y_1 \ \dots \ y_5]$ for a given training image.

3.3.3 Modeling The EXIF-Image Correlation in Linear Regression

As mentioned earlier, the photon transfer curve in [141, 142] shows a correlation between standard deviation of sensor noise and DCSI. We observe from the photon transfer curve plot that when DCSI is represented in the log scale, the large central portion of the photon transfer curve tends to be linear alike. The logarithm of DCSI is linearly associated with our selected EXIF header features and the standard deviation of sensor noises can be represented by our noise features. In this subsection, we correlate each EXIF header feature with the image statistical noise features. Each EXIF header feature is formulated as weighted combination of our reconstructed noise features. For instance, the aperture value y_{p1} of the p -th image is written as follows:

$$y_{p1} = \sum_{x_{pi} \in \mathbf{x}_p} x_{pi} w_{i1} + e_{p1} \quad (3.11)$$

where e_{p1} is the regression error, w_{i1} is the weight of the i -th feature x_{pi} , $x_{pi} \in \mathbf{x}_p$ and $\mathbf{x}_p$ is the extracted noise feature vector.

Since not all features are equally important and some can even adversely affect the modeling accuracy, we need to select significant features by reducing the feature dimensions. Feature selection and feature extraction are two ways to reduce feature dimensions. Here we choose feature selection instead of feature extraction. The reason is that feature selection keeps the information that which single feature in the original 24 dimensional feature vector is more significant and selected, while feature extraction loses this information due to its transformative projection operation from the original feature space onto a new feature space. Thus, sequential floating forward selection (SFFS) [146] is used here. Starting from an empty feature set, SFFS performs stepwise feature inclusion and conditional feature removal to select a subset of features to get significant feature subset. The criteria we minimize in SFFS is the root mean square regression error (RMSRE) of the estimated aperture values on the training images. During each step, the regression weights are estimated using a standard least squares solution in order to estimate the RMSRE.

Figure 3.11: RMSRE versus selected features number in SFFS for estimating aperture value.

Figure 3.11 plots the RMSRE of the estimated aperture value versus the number of selected noise features. When no feature is selected, the RMSRE is about 4.8, which is also the root mean square of the aperture values of all the training images. With

increasing number of selected features, the RMSRE gradually decreases. When the number of selected noise features exceeds 10, the RMSRE almost saturates at 0.78. Therefore, we choose $S=10$ features. In the SFFS selection, the reduction of the RMSRE from 4.8 to 0.78 shows that the aperture value can be efficiently predicted from the selected noise features using our proposed model.

After processing all training images, a set of compact features are obtained. Furthermore, considering the selected noise features, regression weights for the aperture value can be computed as follows:

$$\mathbf{w}_1 = (\mathbf{X}_1^T \mathbf{X}_1)^{-1} \mathbf{X}_1^T \mathbf{y}_1 \quad (3.12)$$

where $\mathbf{X}_1 = \begin{bmatrix} x_{11} & \cdots & x_{1S} \\ \vdots & \ddots & \vdots \\ x_{P1} & \cdots & x_{PS} \end{bmatrix}$, $\mathbf{y}_1 = \begin{bmatrix} y_{11} \\ \vdots \\ y_{P1} \end{bmatrix}$, $x_{Ps} \in \mathbf{x}_p$ is the S -th selected feature by

SFFS and $s \leq S$.

Using the same procedures described, we can learn the regression weights for other EXIF header features. Finally, regression weights $\mathbf{w}_j$, where $j = 1, \dots, 5$, are obtained and saved for the testing phase.

3.3.4 Detection of Image Manipulation

The procedures of detecting image manipulation using the learned regression weights $\mathbf{w}_j$ are shown in Figure 3.12. The selected statistical noise features, $\mathbf{x}^{(j)T}$, are extracted from a testing image in the same manner as the training images.

The absolute numerical difference is computed by using

$$|e_j| = |y_j - \mathbf{x}^{(j)T} \mathbf{w}_j| \quad (3.13)$$

where y_j is the genuine EXIF header feature, and $\mathbf{x}^{(j)T} \mathbf{w}_j$ is the estimated EXIF header feature.

Figure 3.12: Detecting image manipulation using each of EXIF header features.

The detection output is determined as follows

$$U_j = \begin{cases} 1 & \text{if } |e_j| \leq \rho_j \\ 0 & \text{otherwise} \end{cases} \quad (3.14)$$

where $j = 1, \dots, 5$. $|e_j|$ is compared against a threshold, ρ_j . If the absolute numerical difference is larger than the threshold, ρ_j , the testing image is regarded as tampered. Otherwise, the image is genuine.

Finally, according to the majority vote rule, we determine whether the test image is manipulated or authentic.

Table 3.1: Key parameters of three cameras.

Camera model	Image resolution	F-number (F)	Exposure time (t in second)	ISO speed rating (I)
Canon 450D	3088×2056 , 4272×2848	$3.5 \sim 22$	$\frac{1}{5000} \sim \frac{1}{4}$	$100 \sim 800$
Canon 10D	3072×2048	$2.8 \sim 11$	$\frac{1}{1600} \sim 20$	100
Olympus E500	3264×2448	$2.8 \sim 16$	$\frac{1}{3200} \sim \frac{1}{5}$	$100 \sim 1600$

3.4 Experiments and Results

In this section, we evaluate the effectiveness of modeling the correlation between image statistical noise features and five different EXIF camera settings in the linear regression algorithm from multiple cameras.

Figure 3.13: Some samples of three different camera images.

3.4.1 Dataset

We set up the database from three cameras for our experiments, which are Canon 450D, Canon 10D and Olympus E500. We collect 1200 default camera JPEG photos in total, with 400 photos from each camera. These photos are captured with different camera settings and cover a large variety of common scenes with different light conditions. Some samples of the dataset are shown in Figure 3.13. They are captured with different camera settings, which record image resolution, f-number, exposure time and ISO speed rating as shown in Table 3.1.

After computing the three EXIF features in the dataset of the three cameras using Eq. (3.6) - Eq. (3.10), Figure 3.14 shows the normalized distributions of aperture value, shutter speed value, ISO speed value, brightness value and exposure value in the dataset of three cameras respectively. The cumulative distribution of aperture value, shutter speed value, ISO speed value, brightness value and exposure value equal to 1 respectively. We can find that the normalized distributions of these 5 EXIF header

features are different. In other words, when photos are taken with good quality, the photographers usually set camera settings at some commonly used stops which result in the difference of the distribution of the camera settings. Among 5 EXIF header features, ISO speed value is mostly concentrated around 5 corresponding to ISO speed rating of 100 in Figure 3.14(c). In view of the high ISO speed rating resulting in brighter image with more noise, photographers prefer to use the low ISO speed rating in practice. Overall, EXIF headers from our database are fairly diversified in the experiments.

Figure 3.14: Camera setting distributions of the dataset. (a) Aperture value distribution (b) Shutter speed value distribution (c) ISO speed rating value distribution (d) Brightness value distribution (e) Exposure value distribution

3.4.2 Image Tampered by Brightness and Contrast Adjustment

There are many ways to adjust brightness and contrast [8, 40] of a digital image, e.g. gamma correction, histogram equalization. In Figure 3.15, we choose three

typical pairs of brightness and contrast adjustment curves, which are defined in the equations below. For simplicity, we let g be a normalized pixel value of an image, where $0 \leq g \leq 1$.

The x -axis represents normalized pixel values of genuine testing images in three color channels and the y -axis axis represents normalized pixel values of tampered image corresponding to the genuine testing image pixel value. The black curve represents the pixel values of the original image. We consider the solid line as a boundary, which means that there is no change in the image. If the curve falls below this boundary line, the image becomes darker or vice versa. If the slope of the curve is less than 1, the contrast becomes lower or vice versa. In our scenario, six curves are used to tamper the genuine testing images.

The first pair of curves mainly adjust the image brightness, as below:

$$G_1(g, \beta) = \begin{cases} 1 & \text{if } g + \beta \geq 1 \\ g + \beta & \text{if } 0 \leq g + \beta < 1 \\ 0 & \text{if } g + \beta < 0 \end{cases} \quad (3.15)$$

where β is the amount of change. If β is positive, the image brightness is increased and vice versa. We chose $\beta = 1/3$ and $\beta = -1/3$ to generate the “Brightness increment” and “Brightness decrement” curves for an image in Figure 3.15, respectively. “Brightness increment” and “Brightness decrement” curves mainly affect the brightness of the images. Figure 3.16(a) and (b) show the examples of a photo tampered by theses two curves separately.

The second pair of curves is on gamma correction, which is mainly used to adjust the image contrast using

$$G_2(g, \gamma) = g^{(\frac{1}{\gamma})} \quad (3.16)$$

where γ is the gamma parameter. If $\gamma > 1$, the image is brightened. If $\gamma < 1$, the image is darkened, especially for the low pixel values. For demonstration purpose, we set “Gamma compression” and “Gamma expansion” with $\gamma = 2.2$ and $\gamma = 1/2.2$ in Figure 3.15, respectively. Gamma correction is a non-linear adjustment to the image. Figure 3.16(c) and (d) show the examples of a photo tampered by “Gamma

Figure 3.15: Mapping curves used for brightness and contrast adjustment.

compression” and “Gamma expansion” respectively.

We name the third pair of curves in Figure 3.15 as S curve and inverse S-curve. The S curve is given by

$$G_3(g, \alpha) = \frac{1}{1 + e^{-\alpha(g-0.5)}} \quad (3.17)$$

where α controls the degree of change. This curve is applied to increase the contrast of the middle-tone pixel values of an image. On the other hand, the inverse S curve of $G_3^{-1}(g, \alpha)$ decreases the middle-tone contrast of an image. The two curves are drawn with $\alpha = 10$. “S curve” and “Inverse S curve” significantly change the contrast in the middle tone of the images. “S curve” is used to decrease the contrast of pixel values above some mid-value while those below some mid-value are increased. “Inverse S curve” is used to increase the contrast of pixel values above some mid-value while those below some mid-value are decreased. Figure 3.16(e) and (f) show the examples of a photo tampered by “S curve” and “Inverse S curve”, respectively.

(a)

(b)

(c)

(d)

(e)

(f)

Figure 3.16: Some examples of an image tampered by brightness and contrast adjustment curves. Images tampered by (a) Brightness increment, (b) Brightness decrement, (c) Gamma expansion, (d) Gamma compression, (e) S curve, (f) Inverse S curve.

3.4.3 Manipulation Detection on An Individual Camera

In this experiment, we detect 6 types of brightness and contrast adjustment. We first collect 400 camera default JPEG photos from an Olympus E500 camera. These

photos are captured in the automatic mode with different camera settings. These images cover a large variety of common scenes. We randomly select 200 photos to learn the regression weights and the other 200 images for testing. Each color channel of the testing image is manipulated separately using the curves in Figure 3.15, which are commonly used by brightness and contrast adjustment. In total, our testing set contains 1400 images, which consists of 200 genuine testing images and 1200 manipulated testing images.

Figure 3.17: ROC curve of five EXIF header features.

In order to fairly classify the genuine class and the tampered class of testing images, we find the equal error rate thresholds in receiver operating characteristics (ROC) curves. As shown in Figure 3.17, we obtain the accuracy rate for each EXIF header feature. The average accuracy rate of each type of tampered images is shown in Table 3.2. For instance, the true positive (TP) rate of Aperture is 89.5%. On the other hand, the true negative (TN) rates of Aperture for Brightness increment, Brightness decrement, S curve, Inverse S, Gamma compression and Gamma expansion are 91.3%, 92.2%, 87.5%, 88.0%, 87.3% and 92.5%, respectively. The average rate of all five EXIF header features are 89.7%.

From the Table 3.2, we can observe that the true positive rates and true negative

rates remain consistently high for all EXIF header features which indicate that our model is fairly accurate. We have conducted this model on several other camera models. Similarly, a rate of 91.0% is achieved for Canon 10D, and 89.3% is for Olympus E500, respectively.

Table 3.2: The performance of Olympus E500 camera for five EXIF header features.

Average Rate=89.7%		Aperture (%)	Shutter (%)	ISO (%)	Brightness (%)	Exposure (%)
True Positive		89.5	89.6	90.5	91.6	89.8
True Negative	Brightness increment	91.3	90.6	89.5	85.8	89.0
	Brightness decrement	92.2	89.0	88.7	87.3	88.5
	S curve	87.5	86.5	87.3	87.3	91.2
	Inverse S	88.0	93.2	89.0	90.5	92.6
	Gamma compression	87.3	91.6	89.4	87.5	92.5
	Gamma expansion	92.5	90.7	92.2	89.0	89.2

3.4.4 Manipulation Detection on Different Camera Brands and Models

In this section, the experiment is conducted to investigate the performance of the proposed method based on multiple camera brands and models. The dataset consists of 1200 images from Olympus 500, Canon 450D and Canon 10D. These three cameras are from different camera brands with different models.

Specifically, we randomly select 600 intact images to learn the regression weights and the other 600 images for testing. Each color channel of the testing image is manipulated separately using the six curves in Figure 3.15, which are commonly used by brightness and contrast adjustment. In total, our testing set contain 4200 images, which consists 600 genuine testing images and 3600 manipulated testing images. By

applying the same experimental procedure, we obtain the results as shown in Table 3.3. The average rate of all five EXIF header are 90.9%. Based on Table 3.3, we find that the EXIF-Image model has ability to detect manipulated images from different camera brands and models.

Table 3.3: Accuracy rate for different EXIF header features on multiple cameras

Average Rate=90.9%		Aperture (%)	Shutter (%)	ISO (%)	Brightness (%)	Exposure (%)
True Positive		92.6	90.3	89.5	88.9	90.1
True Negative	Brightness increment	89.4	90.4	92.3	93.9	89.4
	Brightness decrement	92.6	90.5	91.5	89.7	92.0
	S curve	88.5	90.5	91.7	89.7	90.8
	Inverse S	90.7	92.5	89.6	90.4	93.1
	Gamma compression	89.7	91.8	91.0	89.7	90.3
	Gamma expansion	92.4	90.1	90.2	92.0	93.6

3.4.5 Detection of Mixed Manipulation Types

In reality, an image forger can manipulate an image in several other color spaces. In our work, we detect the presence of brightness and contrast adjustment without the prior knowledge of the type of brightness and contrast adjustment and the color space in which the manipulation is carried out. We generate manipulated images in three different color spaces including *RGB*, *YCbCr* and *HSI*. In order to detect brightness and contrast adjustment in different color spaces, we perform the following experiment on the same dataset used here. The curves in Figure 3.15 are used to generate the manipulated images in the three different color spaces. All channels in *RGB*, *Y* channel in *YCbCr*, and *I* channel in *HSI* are adjusted accordingly with the six curves of manipulations. In total, we compile 1200 intact images and $1200 \times 6 \times 3 = 21600$

manipulated images. We randomly select 600 intact images and the corresponding 10800 manipulated images to learn the weights and the thresholds, The remaining images are used for testing. Using our learned model to detect brightness and contrast adjustment based on j , $j = 1, \dots, 5$ regarding each EXIF feature, we achieve the average accuracy of all five EXIF results is 88.5%. The performance of our proposed method indicates that our model can reliably detect the presence of brightness and contrast adjustment in different color spaces.

3.5 Summary

In this chapter, based on the photon transfer curve, we establish the relationship by relating image noise statistical features to the EXIF header features using the least-squares solution. We propose a novel method to model the EXIF-Image correlation for image manipulation detection. The model correlates the image statistical noise features with five EXIF header features. First, we use the linear regression algorithm to obtain the correlation between the image statistical noise features and EXIF header features. Then, we make use of the model to detect brightness and contrast adjustment. By applying this model to detect brightness and contrast adjustment, we can achieve more than 89.3% accuracies in three different cameras for six types of brightness and contrast adjustment. The performance shows that our method effectively models the correlation between the image and its EXIF for detecting image manipulation.

Chapter 4

Estimating EXIF Parameters for Image Manipulation Detection

In Chapter 3, five EXIF header features are exploited for image forensics analysis by correlating with image statistical noise features in the linear regression algorithm. In this chapter, a novel EXIF-Image model is established through the non-linear regression by incorporating the first-order and second-order noise features in order to cater the non-linear relationship in the photon transfer curve. Furthermore, different from five EXIF header features used in Chapter 3, the refined EXIF header features include only aperture, shutter speed and ISO speed rating for computation, where brightness value and exposure are removed due to their linear relationship and little performance gain for manipulation detection. Through this, the redundant computation is avoided. The experimental results demonstrate the effectiveness of the proposed EXIF-Image model, even on the real-world forgery images.

4.1 Introduction

Prior works that detected similar brightness and contrast manipulations mainly analyzed the forensics clues on the image only. For instance, Popescu *et al.* [8] modeled luminance nonlinearities with a simple parameter of gamma correction. Cao *et al.* [77] identified gamma correction of digital image operations using peak-gap feature

pattern. Both methods detect the manipulated images operated by a single form of manipulation, i.e. gamma correction. Stamm's method in [40] is capable to globally detect multiple forms of contrast operation using a histogram of pixel value mapping. The model was further applied to localize contrast enhanced image regions. Although the works in [8, 40, 77] discussed the detection of contrast adjustment, their methods cannot effectively detect image brightness adjustment, which may not always be applied together with the contrast adjustment. Avcibas *et al.* [147] proposed a classifier-based method using image quality measure, which was further extended by Bayram *et al.* [9], through introducing additional statistical features, such as binary similarity measures and higher order wavelet statistics. The variations of these features are learnt to detect various image manipulations including brightness and contrast changes. Swaminathan *et al.* [43] suggested a deconvolution-based method to estimate the manipulation filter parameters on color interpolation coefficients to detect various image manipulations including contrast adjustment. However, these works either did not report any results [43] or reported only about 88% accuracy [9, 147] for the challenging task of detecting pure image brightness adjustment.

In this chapter, we model the correlation between the EXIF header and the image noise features and demonstrate its effectiveness in detecting both brightness and contrast adjustments without a prior knowledge of the type and the parameter of the adjustment performed. Due to the ubiquity and the pertinence of the EXIF header corresponding to a JPEG photo, several works that use the EXIF header parameters to assist the forensics analysis have emerged. In detecting photo composite of people, Johnson and Farid [56] required the focal length parameter from the EXIF header to estimate the principal point location from the image of eyes. Kee *et al.* [41] extracted a 576-dimensional camera signature including eight extracted EXIF values for deterministic image authentication. These eight features characterize the EXIF header format, which is supposedly common for cameras of the same model. In the scenario of image authentication, for example, when the camera make/model name is changed in an attempt to conceal the camera source, the extracted signature would become

inconsistent with the known authentic camera signature. Although image manipulation often causes detectable header changes, we note that Kee’s method does not directly authenticate the image content. Hence, it would not work in the scenario that a forger deliberately keeps the header intact after manipulating the image content. However, these works in [41, 56] mainly utilize a few selected EXIF parameters or the EXIF standard format to facilitate the forensics analysis. Different from these works and the EXIF parameters used, we model the correlation between several camera shot settings in the EXIF header and statistical image noise features. When an image is manipulated, the EXIF-Image correlation can be destroyed. We observe that the numerical differences between the actual EXIF features and their corresponding estimated EXIF features from the noise features can serve as an excellent indicator to determine whether an image represents the original camera recording or it has gone through the brightness and contrast adjustment. Since such adjustments are quite common in forgery as well as in non-deceptive image manipulation, our method can be used to strengthen the claim that an image with an intact EXIF header is indeed an original camera output because its aperture/shutter/ISO settings match with its noise statistics.

This chapter is organized as follows. Section 4.2 details the extraction for statistical image noise features and EXIF features. After feature extraction, we model the EXIF-Image correlation between the selected noise features and each EXIF header feature using the nonlinear regression for discriminating the intact images from the manipulated images. In Section 4.3, a set of experiments demonstrate the effectiveness of our learned EXIF-Image correlation for image manipulation detection. Section 4.4 concludes this chapter.

4.2 Proposed Manipulation Detection Framework

As mentioned before, the photon transfer curve in [141, 142] shows a phenomenon that the standard deviation of total noise is correlated with digital camera signal

Figure 4.1: Extraction of image statistical noise features.

intensity (DCSI), i.e. the amount of effective light photons impinging onto a sensor during the shutter-opening period. Knowing that the amount of total noise can be approximated from the image and DCSI is traditionally estimated from several shot settings like aperture size, exposure time and ISO in EXIF headers, the photon transfer curve suggests a possible correlation between the image and its EXIF header parameters. To investigate this, our proposed model correlates several selected EXIF features with the statistical image noise features. Below, we describe the extraction of statistical image noise features and the corresponding EXIF header features.

4.2.1 Extraction of Image Noise Features

Image noise features are extracted in the same way as in Chapter 3. We summarize extraction of image noise features based on four types of denoising filters as shown in Figure 4.1. In view that the sharp area of the image tends to have high frequency energy which affects the noise estimation, we compute mean and standard deviation of noise features based on the non-sharp image area. A non-sharp area is defined by the sharpness residuals. Knowing that different denoising filters are effective in removing different types of image noises [97], we choose a set of denoising filters including averaging filter, Gaussian filter, median filter and Wiener filter for extracting different types of residuals. For example, averaging filter and Gaussian filter are good for removing high-frequency noise, median filter is effective for removing the salt and

pepper noise and Wiener filter removes the noise associated with the local pixels. Totally, a 24 dimensional feature vector is formed from each image $\mathbf{A}$ for $3 \times 4 = 12$ combinations of color channels and denoising filters.

4.2.2 Extraction of EXIF Header Features

We compute three EXIF header features [145] associated with DCSI as follows:

$$\begin{aligned} \text{Aperture:} \quad y_1 &= \log_2(F^2) \\ \text{Shutter speed:} \quad y_2 &= \log_2\left(\frac{1}{t}\right) \\ \text{ISO speed rating:} \quad y_3 &= \log_2\left(\frac{I}{3.125}\right) \end{aligned} \tag{4.1}$$

where F is f-number, t is exposure time and I is ISO speed rating. These EXIF header features share a common unit of *stop*, where increment by 1 *stop* indicates the amount of effective light falling on the image sensor is doubled.

4.2.3 Modeling the EXIF-Image Correlation in Non-linear Regression

As mentioned earlier, the photon transfer curve [141, 142] depicts a correlation between the amount of total noise and DCSI. When the standard deviation of total noise and DCSI are represented in log scale, we observe that a large central portion of the photon transfer curve forms a linear-alike correlation. As majority of photos are non-saturated with its DCSI residing in the central portion of the photon transfer curve, this linear-alike correlation is expectedly applicable to a wide range of ordinary photos. Here, the logarithm of DCSI is linearly associated with our selected EXIF features and logarithm of the number of total noise can be approximated from our noise features computed from the non-sharp image area. In this section, we model the correlation between each EXIF header feature and our selected noise features using a set of images for manipulation detection.

Figure 4.2(a) shows the block diagram for modeling the EXIF-Image correlation. Let $\mathbf{z}_1, \dots, \mathbf{z}_P$ be the image noise feature vectors extracted from a set of P

Figure 4.2: Block diagram of the proposed method.

intact images and $\mathbf{z}_{(P+1)}, \dots, \mathbf{z}_{(P+Q)}$ be the vectors from Q manipulated images. Correspondingly, we let $\mathbf{y}_1, \dots, \mathbf{y}_P$ be the EXIF feature vectors from the intact class and $\mathbf{y}_{(P+1)}, \dots, \mathbf{y}_{(P+Q)}$ be the vectors from the manipulated class. Here, $\mathbf{z}_p = \{z_{pi} | i = 1, \dots, C\}$ and $\mathbf{y}_p = \{y_{pj} | j = 1, \dots, J\}$ form a pair of image feature vector and EXIF feature vector for the p -th image. $C = 24$ and $J = 3$ are the dimensions of the image and the EXIF feature vectors respectively. We separately study the correlation between each of the three EXIF features with the image noise features. Suppose y_{pj} is the j -th EXIF feature of the p -th image from the intact class, we write

$$y_{pj} = \sum_{i=1}^{S_j} x_{pi} w_{ij} + e_{pj} = \mathbf{x}_p^{(j)T} \mathbf{w}_j + e_{pj} \quad (4.2)$$

where e_{pj} is the numerical difference, w_{ij} is the weight of the i -th new feature x_{pi} . $\mathbf{x}_p^{(j)} = \{x_{pi} | i = 1, \dots, S_j\}$ is a vector of our selected S_j features from $\mathbf{x}_p$, $\mathbf{x}_p = [z_{p1}, \dots, z_{pC}, \dots, z_{p1}z_{p2}, z_{p1}z_{p3}, \dots, z_{p(C-1)}z_{pC}, \dots, z_{p1}^2, \dots, z_{pC}^2]^T$ denotes our new feature vector, which includes both the first-order and the second-order polynomials of our noise features. The second-order polynomials are added to cater for nonlinearity of the underlying correlation due to various digital processing of a

camera system. $\mathbf{w}_j = \{w_{ij} | i = 1, \dots, S_j\}$ is a vector of the corresponding weights. For each intact image, we can produce an equation similar to Eq. (4.2). In matrix representation, we have

$$\mathbf{e}_j = \mathbf{y}_j - \mathbf{X}_j \mathbf{w}_j \quad (4.3)$$

where $\mathbf{e}_j = \begin{bmatrix} e_{1j} \\ \vdots \\ e_{Pj} \end{bmatrix}$, $\mathbf{y}_j = \begin{bmatrix} y_{1j} \\ \vdots \\ y_{Pj} \end{bmatrix}$, $\mathbf{X}_j = \begin{bmatrix} [\mathbf{x}_1^{(j)}] & \dots & [\mathbf{x}_P^{(j)}] \end{bmatrix}^T$, $\mathbf{w}_j = \begin{bmatrix} w_{1j} \\ \vdots \\ w_{S_j j} \end{bmatrix}$. Suppose

$P \gg S_j$, i.e. sufficient number of intact images are given, we solve $\mathbf{w}_j$ as the least squares solution below to yield:

$$\min(\|\mathbf{e}_j\|^2) \implies \mathbf{w}_j = (\mathbf{X}_j^T \mathbf{X}_j)^{-1} \mathbf{X}_j^T \mathbf{y}_j \quad (4.4)$$

Correspondingly, our absolute numerical difference for the p -th image is computed using

$$|e_{pj}| = |y_{pj} - \mathbf{x}_p^{(j)T} \mathbf{w}_j| \quad (4.5)$$

where $1 \leq p \leq (P + Q)$.

Note that before the weight estimation, we apply feature selection technique to search for a compact feature subset instead of using the full set of image features directly. This is because by including the second-order terms, our image feature dimension increases significantly from C to $C + \binom{2}{C} + C = \frac{C(C+3)}{2}$, which requires more intact images to estimate a larger number of weights and also undesirably increases our computational complexity. Since not all the image features perform equally well and some even adversely affect the outcome, we apply sequential floating forward selection (SFFS) [146] in conjunction with Fisher's criterion to select our feature subset. Initializing from an empty feature set $\mathbf{x}_p^{(j)} \in \emptyset$, SFFS [146] performs stepwise feature inclusion and conditional removal using floating search to find a best subset of features based on a user-defined goal. In this chapter, we choose to maximize Fisher's Ratio as our goal to discriminate the intact class from the manipulated class. Generally, we expect small difference for the intact image in the case that a strong correlation is present between the j -th EXIF feature and our selected image features.

As image manipulations can weaken or even destroy this EXIF-Image correlation, we expect enlarged difference for the manipulated image. As intact training images and manipulated training images are both available, Fisher's Ratio as a different criterion is adopted here instead of the regression mean squared error in chapter 3, which is capable for two classes classification. Specifically, when the absolute numerical difference is used to differentiate the intact and the manipulated classes, we compute Fisher's Ratio using

$$T_j = \frac{(\mu_{1j} - \mu_{0j})^2}{\sigma_{1j}^2 + \sigma_{0j}^2} \quad (4.6)$$

where

$$\begin{aligned} \mu_{1j} &= \frac{1}{P} \sum_{p=1}^P |e_{pj}|, & \sigma_{1j}^2 &= \frac{1}{P-1} \sum_{p=1}^P (|e_{pj}| - \mu_{1j})^2 \\ \mu_{0j} &= \frac{1}{Q} \sum_{p=P+1}^{P+Q} |e_{pj}|, & \sigma_{0j}^2 &= \frac{1}{Q-1} \sum_{p=P+1}^{P+Q} (|e_{pj}| - \mu_{0j})^2 \end{aligned} \quad (4.7)$$

As a larger Fisher's Ratio represents more discrimination between the intact and manipulated classes, we determine our best number of selected features corresponding to the maximal T_j when the size of our selected features $\mathbf{x}_p^{(j)}$ is dynamically increased in SFFS process.

4.2.4 Image Manipulation Detection

After modeling the EXIF-Image correlation for all three EXIF features, we use our outcomes to detect the manipulated image as shown in Figure 4.2(b). Given a test image, we first compute its image features and the EXIF header features. For each EXIF feature y_j , we compute its difference

$$|e_j| = |y_j - \mathbf{x}^{(j)T} \mathbf{w}_j| \quad (4.8)$$

based on our selected features $\mathbf{x}^{(j)}$ and their weights $\mathbf{w}_j$. The absolute difference $|e_j|$ is linearly normalized to the range of [0,1] from its original range [MIN, MAX] of the training set, which is followed by a score-level fusion as below.

$$u = \prod_{j=1}^3 \text{normalize}(|e_j|) \quad (4.9)$$

In Chapter 3, when using the voting rule for final detection decision, three ROC curves of aperture, shutter speed and ISO in the EXIF header are needed to learn their corresponding thresholds. Although more than 89.3% accuracies are achieved, learning multiple thresholds for different ROC curves is not desirable. Consequently, the sum of the normalized regression errors is performed to generate one single ROC curve and to derive only one threshold in Chapter 4.

Our detection outcome for combining the three EXIF features is computed as

$$U = \begin{cases} 1 & \text{if } |u| \leq \rho \\ 0 & \text{otherwise} \end{cases} \quad (4.10)$$

Here, $U = 1$ denotes the intact class and $U = 0$ is for the manipulated class. The threshold ρ is chosen to maximize the average of true positive (TP) rate and the true negative (TN) rate on the dataset. TP and TN are the classification accuracy rates for the intact class and the manipulated class, respectively. By computing the average accuracy for the two classes for selecting the best threshold, we place equal emphasis on the two classes. The selected threshold is used in the test scenario to determine whether an unseen image is manipulated.

4.3 Experiments and Results

4.3.1 Detection of Individual Manipulation Curve

In this section, we evaluate the performance of our proposed method for detecting individual brightness and contrast adjustment curve.

1. Dataset

We set up the image dataset from the three different cameras, which are Canon 450D, Canon 10D and Olympus E500. We collect 1200 default JPEG photos in total, with 400 photos from each camera.

We generate the manipulated images using the six curves as shown in Figure 4.3.

Figure 4.3: Brightness and contrast adjustment with small changes.

These six curves have more subtle changes than the six curves mentioned in Chapter 3. The reason we choose these six curves is that less change is supposed to be more difficult for image manipulation detection. In *RGB* color space, each color channel of an intact image is manipulated separately using each curve. As such, we obtain a total of $1200 \times 6 = 7200$ manipulated images. Including the intact images, our entire dataset consists of 8400 images. Then we randomly select 600 intact images and their corresponding 3600 manipulated images for selecting the features and for determining the weights and the thresholds. The remaining 4200 images are used for testing.

2. Determining The Number of Selected Features

All our selected denoising filters have a window size 3×3 for the statistical image noise feature computation. The standard deviation for Gaussian filter is chosen as 0.5. By including additional second-order polynomial features from the 24 extracted image noise features, we generate a new feature vector of 324 dimensions including both the first-order and the second-order noise features. As mentioned early, we adopt SFFS to select a compact set of noise features using Fisher's Ratio as the criterion

(a)

(b)

(c)

Figure 4.4: Fisher's Ratio distributions against number of selected features for estimating aperture value in terms of different curves of (a) Brightness decrement (b) Gamma expansion (c) S curve.

in Eq. (4.9) and Eq. (4.10). As an example in Figure 4.4(a), we plot Fisher's Ratio against the number of selected features for the EXIF aperture feature where manipulated images are generated using the "Brightness decrement" curve. It shows that the Fisher's Ratio increases to a maximum and then decreases gradually when

Figure 4.5: The numerical difference distributions of the intact testing images and the manipulated testing images of Brightness decrement in (a), Gamma expansion in (b), S curve in (c).

the number of selected features increases. When 40 features are selected, Fisher's Ratio achieves the maximum. We then utilize a compact set of 40 selected features for estimating EXIF aperture value.

Using our selected set of features for predicting the same EXIF aperture feature, Figure 4.5(a) shows the distribution of numerical differences for the intact testing images and the brightness decrement testing images where the differences of the intact testing images are smaller than the differences of the manipulated testing images. Based on the Fisher’s Ratio plots in Figure 4.4(b) and 4.4(c), 33 and 24 noise features are selected for detecting the “Gamma expansion” and “S curve” manipulations respectively. Furthermore, the distributions of numerical differences for these curves are plotted in Figure 4.5(b) and 4.5(c) respectively. We can see that the manipulated class is largely separated from the intact class in Figure 4.5(a-c) using our selected feature subsets.

Table 4.1: The performance comparison for different manipulation curves.

Manipulation curves		Proposed Method (%)								Stamm [40](%)	
		Aperture		Shutter		ISO		Combined		TP	TN
		TP	TN	TP	TN	TP	TN	TP	TN		
Brightness	Brightness increment	99.6	100	99.8	99.7	100	99.9	99.7	100	45.5	56.8
	Brightness decrement	100	100	99.8	99.8	100	100	99.8	99.8	68.3	54.8
	Average accuracy	99.9		99.8		99.9		99.8		56.4	
Contrast	S curve	100	99.3	100	99.0	100	99.3	99.8	99.5	99.6	100
	Inverse S	99.7	99.8	100	99.2	99.0	99.0	100	99.2	99.6	99.1
	Gamma compression	99.8	99.3	99.8	99.7	97.7	97.3	100	99.5	99.6	100
	Gamma expansion	99.8	99.2	100	99.8	99.0	97.3	100	99.8	99.6	100
	Average accuracy	99.6		99.7		98.6		99.7		99.7	

3. Detection Accuracy

We evaluate the manipulation detection performance using each individual EXIF feature by plotting the ROC curves corresponding to the six manipulation curves in Figure 4.3. For example, Figure 4.6 shows the enlarged ROC curves for the EXIF aperture feature. From this figure, we can observe that equal error rates for six curves of brightness and contrast adjustment are less than 2%. Table 4.1 shows

the performance comparison of our method with Stamm’s method [40] in terms of TP and TN. For instance, using the aperture value, we find that the TP and TN are 99.6% and 100% for the “Brightness increment” manipulation. The TP and TN rates of the remaining EXIF-Image models for “Brightness increment” curve are greater than or equal to 99.7%. By combining all detection results using Eq. (4.9) and Eq. (4.10), we achieve 99.7% TP rate and 100% TN rate without requiring any prior knowledge of the manipulation type. The average accuracy rates remain high consistently for all three EXIF features which validates the effectiveness of our model. For detection of the image brightness adjustment, our method achieves a significantly better average accuracy of 99.8% since Stamm’s method only focuses on contrast manipulation detection. For the four types of contrast adjustment, our overall accuracy after combining three EXIF features is 99.7%, which is similar to Stamm’s method [40]. The proposed EXIF-Image model is also effective for other color space like $YCbCr$ and HSI .

Figure 4.6: Zoomed-in ROC curves for EXIF aperture value corresponding to six curves of brightness and contrast adjustment.

To analyze the factors that cause the detection errors, we examine the wrongly classified images. Out of the 0.2% wrongly classified testing images for two brightness curves and the 0.3% wrongly classified testing images for four contrast curves,

we find that 0.5% total wrongly classified images for six curves are mainly associated with extreme and rare EXIF values. Our training dataset lacks the samples with such extreme EXIF values, which makes the comprehensive EXIF-image modeling and reliable manipulation detection almost impossible for such images. For instance, 47.1% of the total errors for estimating aperture are contributed by the low aperture value of 3, which corresponds to an f-number of 2.8. To reduce the error rate, we can construct a dedicated EXIF-Image model for the aperture value of 3. Specifically, we perform a test with 600 images are taken under the aperture value of 3 by Olympus E500. We randomly select 400 images for determining the EXIF-Image model and the remaining images for testing. Following the same process, we obtain high TP of 95.5% and TN of 100% for estimating aperture as shown in Table 4.2. Table 4.2 also tabulates our testing results for several other EXIF parameter combinations. Our experimental results show that the EXIF-Image model for a specific EXIF combination works well, even if their values are in the extreme range. For achieving better result, we can therefore perform model selection to use the dedicated model for authentication if the EXIF value falls into the extreme range.

Table 4.2: The performance comparison for the images from fixed camera settings.

Camera settings	Aperture(%)		Shutter(%)		ISO(%)		Combined(%)	
	TP	TN	TP	TN	TP	TN	TP	TN
2.8, $\frac{1}{125}$, 100	95.5	100	95.5	100	95.5	100	98.0	100
5.6, $\frac{1}{125}$, 100	99.5	99.7	99.5	99.7	99.5	99.7	99.5	99.8
11, $\frac{1}{125}$, 100	99.5	99.9	99.5	99.9	99.5	99.9	99.5	99.7
5.6, $\frac{1}{30}$, 100	99.5	100	99.5	100	99.5	100	99.5	100
5.6, $\frac{1}{1000}$, 100	99.0	99.7	99.0	99.7	99.0	99.7	99.0	99.7
5.6, $\frac{1}{125}$, 400	100	99.7	100	99.7	100	99.7	100	99.8

4. Comparison with Linear Regression Model

We repeat our experiment by employing the linear regression algorithm and compare the performance for both the linear and nonlinear regression algorithms to evaluate the gain of the second-order polynomial noise features inclusion. The comparison of the nonlinear regression and the linear regression one is performed on the same feature pool by using the same feature selection method. Only Fisher’s Ratio for SFFS in Chapter 4 is used in the experiment to achieve fair comparison of this nonlinear regression with the linear regression one. Our average accuracies are 89.6% and 93.2% to detect the same kind of brightness and contrast adjustment, respectively, in the linear regression model. The average accuracies for detecting the same kind of brightness and contrast adjustment are 10.2% and 6.5% poorer than using our proposed nonlinear regression model. This result shows that incorporating the second-order image noise features is effective to improve the manipulation detection performance.

5. Predictions of Aperture and Shutter Speed

Based on our proposed framework, we study the accuracy of the aperture and shutter speed predictions when DCSI is held constant. As mentioned early, DCSI is the amount of effective light photons impinging on the sensors during the shutter-opening period, which can be represented using the following formula [141]:

$$S = \psi S_V \xi \quad (4.11)$$

where ψ is the average number of incident photons per pixel, which is associated with the aperture and shutter speed settings; S_V is the sensitivity of the sense node (V/e.), which is related to the ISO speed rating setting; ξ denotes a constant for the given type of sensor. Note that images captured with the same DCSI but varying aperture and shutter speed values on the same scene are visually identical. It is thus a challenging task to predict the aperture or shutter speed from image noise features. We do not predict the ISO in this section as ISO is closely relevant to the amount of noise and its prediction from noise features is a relatively simple task as compared with predictions of aperture and shutter speed. Below, we show two sets

of the experiments in details.

Figure 4.7: Aperture predictions for the images from the same camera with the equivalent DCSI by varying different settings of aperture value (Av) and shutter speed value (Sv), respectively. Aperture predictions for (a) intact images and (b) manipulated images by brightness decrement.

In the experimental setup, we take 1800 intact images from Olympus E500 camera with 600 images from each of three different combinations of aperture value (Av) and shutter speed value (Sv) but a constant DCSI. The captured images have the equivalent exposure value of 10 stops with the following three combinations: (1) Av=3

Figure 4.8: Shutter speed predictions for the images from the same camera with the equivalent DCSI by varying different settings of aperture value (Av) and shutter speed value (Sv), respectively. Shutter speed predictions for (a) intact images and (b) manipulated images by brightness decrement.

and $Sv=7$, (2) $Av=4$ and $Sv=6$, (3) $Av=5$ and $Sv=5$. Firstly, 300 randomly selected images from each of three combinations are compiled to 900 training images to model the EXIF-Image correlation, followed by the test predictions of the aperture and shutter speed using the remaining images. Figure 4.7 shows the predicted aperture values for different combinations of aperture and shutter speed settings. For instance, Figure 4.7(a) shows the predicted aperture values for the intact training and testing

images, where x -axis denotes the image index and y -axis is the predicted aperture value. The predicted aperture values in red color (the one with the symbol “+”) from 900 training images concentrate at around the ground-truth levels for $A_v=3$, 4 and 5. For test images, we observe their predicted values are also closely centered around ground-truth of aperture values with small divergence. We find that although the aperture values of the intact images are not perfectly estimated, the prediction of the intact images are closer compared with the aperture prediction of the manipulated images in Figure 4.7(b). Figure 4.8(a) and (b) show the similar results for predicting shutter speed with different S_v settings. Based on the experimental results in Figure 4.7 and Figure 4.8, we find that when DCSI is held constant, aperture and shutter speed settings of the training and testing images from the same camera can be closely predicted using our proposed noise features, and our modelling and prediction framework.

In addition, we also conduct the experiments on the images captured from multiple cameras. In particular, we take 900 images from each of Olympus E500 and Canon 550D cameras using a constant DCSI in the experimental setup. Specifically, the images have the equivalent exposure value of 10 stops with the following three combinations of aperture value (A_v) and shutter speed value (S_v): (1) $A_v=3$ and $S_v=7$, (2) $A_v=4$ and $S_v=6$, (3) $A_v=5$ and $S_v=5$. Firstly for each combination, 300 randomly selected Olympus images are compiled to 900 training images to model the EXIF-Image correlation. This is followed by measuring the predictions of the aperture and shutter speed, respectively, using 900 Canon images as the testing images. Figure 4.9 shows the predicted aperture values for different combinations of aperture and shutter speed settings. For instance, Figure 4.9(a) shows the predicted aperture values for the intact training and testing images, where x -axis denotes the image index and y -axis is the predicted aperture value. The predicted aperture values in red color (the one with the symbol “+”) from 900 training images concentrate at around the ground-truth levels for $A_v=3$, 4 and 5. For test images, we observe that their predicted values are centered around the ground-truth levels with small

Figure 4.9: Aperture predictions for the images from different cameras with the equivalent DCSI by varying different settings of aperture value (Av) and shutter speed value (Sv), respectively. Aperture predictions for (a) intact images and (b) manipulated images by brightness decrement.

divergence. We find that although the aperture values of the intact images are not perfectly estimated, the prediction of the intact images are closer compared with the aperture prediction of the manipulated images in Figure 4.9(b). Furthermore, the similar results for predicting shutter speed with different Sv settings as shown in Figure 4.10. Our results in Figure 4.9 and Figure 4.10 show the possibility of predicting three commonly used combinations of aperture and shutter speed settings using our

Figure 4.10: Shutter speed predictions for the images from different cameras with the equivalent DCSI by varying different settings of aperture value (A_v) and shutter speed value (S_v), respectively. Shutter speed predictions for (a) intact images and (b) manipulated images by brightness decrement.

proposed noise features and estimation model when DCSI is held constant.

6. Performance on Wide Range of Parameter Settings

We study here the manipulation detection performance for a wide range of brightness and contrast adjustment with different β , γ and α settings in Eq. (3.15), Eq. (3.16) and Eq. (3.17). We generate the manipulated images from the intact images

using each of different parameter settings as shown in Figure 4.11(a-f).

Figure 4.11: Sensitivity analysis of manipulation detection performance for $G_1(g, \beta)$, $G_2(g, \gamma)$, $G_3(g, \alpha)$ and $G_3^{-1}(g, \alpha)$ curves.

Specifically, 600 randomly selected intact images from the same dataset as before

and $600 \times 6 = 3600$ manipulated images for 6 different β parameters in Figure 4.11(a) are used for determining the EXIF-Image model. The remaining images are applied for testing. Following the same process, we plot the average accuracy of TP and TN for combining the three EXIF features as a function of the adjustment curve parameters in Figure 4.11(a). Figure 4.11(a) shows that when the value of β decreases to $\frac{1}{20}$, our average accuracy of the combined detection based on three EXIF features drops to about 84.5%. As mentioned earlier, the smaller β represents the less brightness increment change in the image. By increasing the image brightness to $\beta = \frac{1}{8}$, the average accuracy becomes as high as 97.0%. Figure 4.11(b-f) show the similar trend. By choosing $\beta = \pm \frac{1}{24}$, $\gamma = \frac{1}{1.05}$ or 1.05 and $\alpha = 2$ of $G_3(g, \alpha)$ and $G_3^{-1}(g, \alpha)$, the average accuracies drop to below 80%, which is below our steady-state accuracy for detecting visually appealing manipulations. However, with such small manipulation strengths, the effect of change is hardly visible to human eyes. Below, we perform the proposed model on one example to investigate the sensitivity of brightness adjustment as shown in Figure 4.12.

For instance, manipulated images in Figure 4.12(a-d) and (f-i) are generated from the intact image in Figure 4.12(e) by changing the image brightness. Among Figures 4.12(d-f), human beings cannot perceive the differences between the intact image in Figure 4.12(e) and the manipulated images in Figure 4.12(d) and (f), which are generated by $G_1(g, \frac{1}{32})$ and $G_1(g, -\frac{1}{32})$. On the contrary, by observing Figure 4.12(i), it appears that Figure 4.12(i) is taken in the evening while Figure 4.12(e) is captured in the daytime. By applying our detection model to Figure 4.12(a-i), we obtain the results in Table 4.3. Compared with the actual and predicted EXIF features, we can confidently differentiate the manipulated images in Figures 4.12(a-c) and (g-i) from the intact image in Figure 4.12(e). But our model cannot detect the manipulated images Figures 4.12(d) and (f). Therefore, practically we only need to test up to the level of changes that can be perceived by human eyes. For the common manipulations to deceive human eyes, our proposed method consistently exhibits the capability of manipulation detection.

Figure 4.12: Images (a-i) with f-number = 5.6, exposure time = $\frac{1}{250}$, ISO = 400. Manipulated images (a-d) and (f-i) are generated from intact image (e) by image brightness changes of $G_1(g, \frac{1}{4})$, $G_1(g, \frac{1}{8})$, $G_1(g, \frac{1}{16})$, $G_1(g, \frac{1}{32})$, $G_1(g, -\frac{1}{32})$, $G_1(g, -\frac{1}{16})$, $G_1(g, -\frac{1}{8})$ and $G_1(g, -\frac{1}{4})$.

Table 4.3: EXIF parameter estimation for the photos in Figure 4.12.

Photo	Aperture (<i>stop</i>)		Shutter (<i>stop</i>)		ISO (<i>stop</i>)	
	EXIF	Predicted	EXIF	Predicted	EXIF	Predicted
(a)	5	-3.5	8	-8.4	7	15.9
(b)		-1.8		4.8		11.9
(c)		4.2		6.2		9.6
(d)		5.0		8.2		8.9
(e)		5.7		8.6		8.1
(f)		6.0		9.1		7.4
(g)		8.5		10.5		5.9
(h)		9.7		16.4		3.6
(i)		12.4		20.3		1.2

4.3.2 Refining The EXIF Header Features

We include the fourth and fifth EXIF features in Chapter 3 as they represent physically meaningful quantities in computation photography. We hope that our modeling process would select the most appropriate image noise features specially tailored to these two EXIF features even though we are aware that these features depend linearly on the first three EXIF features.

Table 4.4: The performance comparisons.

Performance (%)	Aperture		Shutter		ISO		Brightness		Exposure	
	TP	TN	TP	TN	TP	TN	TP	TN	TP	TN
Five EXIF header features	99.8	99.3	100	99.5	99.7	99.2	99.7	93.6	99.7	99.3
Three EXIF header features	99.8	99.3	100	99.5	99.7	99.2	99.8	99.1	99.8	99.5

We have conducted a new test, which replaces the regression models for the fourth and fifth EXIF features with the corresponding combination of models determined from the first three EXIF features. In the experiment, we compare three EXIF header features with our previous method by using five EXIF header features as illustrated in Table 4.4. Compared with our previous TP of 99.7% and TN of 93.6% for estimating brightness, the new TP and TN we obtained based on the linear relationship among three EXIF header features (aperture, shutter speed and ISO) are 99.8% and 99.1%, respectively. Similarly, compared with our previous TP of 99.7% and TN of 99.3% for predicting exposure, TP and TN based on the combination of two EXIF header features (aperture and shutter speed) achieve 99.8% and 99.5%. As the results are fairly similar, we consider that they do not add new information and remove the fourth and fifth EXIF features in the EXIF-image modeling.

4.3.3 Manipulation Detection without Knowing The Camera Source

We have investigated the effectiveness of the EXIF-Image model for manipulation detection without the knowledge of the camera brand/model. Three experiments are conducted as follows. We take 1200 intact images from three camera brands, with 400 each from Canon 450D and Olympus E500 cameras, and 200 each from the Sony A350 and Sony S930 cameras. Then $400 \times 6 = 2400$ manipulated images for each of three camera brands are generated by six curves as shown in Figure 4.3 in all channels of *RGB* color space. In total, $400 + 400 \times 6 = 2800$ images for each of three camera brands are collected. The training images for modeling the EXIF-Image correlation are taken from two of the three camera brands but the testing images are from the third camera brand. For instance, $800 + 800 \times 6 = 5600$ images from Canon and Olympus are used to determine the EXIF-Image model. Then $400 + 400 \times 6 = 2800$ images from Sony are for testing. Following the same experimental process, we obtain the results in Table 4.5. We achieve the average accuracy of 99.8% through combining the three detection results. Similarly, the average accuracies of combining the three detection results are 99.2% and 98.1% for the other two different combinations of the images sources. Based on the three different camera brands, the experimental results show that our EXIF-Image model performs accurately in a blind mode without the prior knowledge of the training camera brand/model.

In addition, we have conducted another experiment. We use the same dataset as the above experiment, where only images from one camera brand are used for determining the EXIF-Image model while the testing images are from another brand. Using different combinations of camera brand, we conduct six experiments in total. Our results are tabulated in Table 4.6. For instance, when the EXIF-Image model is first determined from the images of Canon, and then applied for the testing images of Olympus, the TP rates regarding the aperture, shutter speed and ISO are 100%, 100% and 99.0% and the TN rates are 99.5%, 97.5% and 100%, respectively. TP and TN after combining the three EXIF feature results are 99.7% and 99.9%. The average

Table 4.5: The performance comparison for the images from different camera sources.

Modeling	Testing	Aperture (%)		Shutter (%)		ISO (%)		Combined (%)		
		TP	TN	TP	TN	TP	TN	TP	TN	Ave.
Canon and Olympus	Sony	99.2	96.3	99.2	97.9	98.8	98.8	99.8	99.8	99.8
Canon and Sony	Olympus	99.2	96.6	97.8	95.1	98.5	96.0	99.7	98.8	99.2
Olympus and Sony	Canon	100	98.6	100	98.0	96.0	97.9	100	96.2	98.1

accuracy of combining the three EXIF features' (i.e. aperture, shutter speed and ISO) results is 99.8%. Among the six experiments with different combinations of the images sources, the average accuracies of combining the three EXIF header features' results are more than 99.5%. The results from the two sets of the experiments demonstrate that our EXIF-Image model can be applied for image authentication without the prior knowledge of the source camera model based on the three different camera brands used in our experiments.

Table 4.6: Performance comparison for the images for modeling from one camera brand and the testing images from the other camera brand.

Modeling	Testing	Aperture (%)		Shutter (%)		ISO (%)		Combined (%)		
		TP	TN	TP	TN	TP	TN	TP	TN	Ave.
Canon	Olympus	100	99.5	100	97.5	99.0	100	99.7	99.9	99.8
Canon	Sony	99.8	99.6	99.3	99.4	99.0	100	99.8	99.8	99.8
Sony	Olympus	100	98.1	100	98.7	98.3	99.9	99.0	99.9	99.5
Sony	Canon	96.8	98.1	99.8	98.5	99.8	99.8	99.8	100	99.9
Olympus	Canon	97.8	99.1	99.3	98.8	99.8	98.3	100	99.8	99.9
Olympus	Sony	99.5	99.8	99.0	98.5	99.0	98.3	99.5	99.8	99.7

Image (a) with f-number = 5.6,
exposure time = $\frac{1}{250}$, ISO = 400.

Image (b) with f-number = 5.6,
exposure time = $\frac{1}{250}$, ISO = 400.

Image (c) with f-number = 5.6,
exposure time = $\frac{1}{125}$, ISO = 100.

Image (d) with f-number = 5.6,
exposure time = $\frac{1}{125}$, ISO = 100.

Image (e) with f-number = 5.6,
exposure time = $\frac{1}{125}$, ISO = 100.

Image (f) with f-number = 5.6,
exposure time = $\frac{1}{125}$, ISO = 100.

Figure 4.13: Manipulated image (b) is generated from intact image (a) by “Brightness decrement”. Composite images (d) and (f) are created by intact images (c) and (e).

4.3.4 Detection of Forgery Photos

Brightness adjustment as a common form of image manipulation can affect the perceptual quality of digital images to fool others in deceiving from the truth. For example in Figure 4.13, images (a-b) contain the same scenery with different brightness. By observing these two images, it appears that (a) is captured in the daytime and (b) is captured in the evening. Visually, it is difficult for one to figure out which of these two images is manipulated. While applying our detection model to these two images, we confidently differentiate the manipulated image from the intact image. We first compute the numerical difference of each of three EXIF features and compare each difference with its corresponding threshold, which is obtained earlier. As shown in Table 4.7, the predicted aperture value in image (a) is 5.7. Compared with the aperture value of 5 in the EXIF header, the difference of 0.7 is smaller than its threshold of 4.8. Similarly, the numerical difference of each of the remaining EXIF header features is compared with the corresponding threshold, respectively. Finally, based on the combined result by Eq. (4.9) and Eq. (4.10), we correctly determine image (a) as intact and image (b) as manipulated by combining three EXIF feature results.

In addition, brightness and contrast adjustment is often used as a part of malicious image content manipulation, e.g. photo composition. Brightness and contrast adjustment can improve the overall perception of a composite image, especially while two images taken under different lighting conditions and surroundings need to be combined. For example, two manipulated images (d) and (f) in Figure 4.13 are created by compositing intact images (c) and (e). The intact images (c) and (e) are first composited in Photoshop, and then brightness and contrast are adjusted to make the manipulated images in (d) and (f) visually acceptable. By observing (d) and (f), it is difficult to recognize the manipulated images using human eyes. However, using our detection model, we compute the numerical difference of each of three EXIF features and compare it with its threshold. Our detection results reliably differentiate that

images (c) and (e) are intact and images (d) and (f) are manipulated.

Table 4.7: EXIF parameter estimation for the images in Figure 4.13.

Photo	Aperture (<i>stop</i>)			Shutter (<i>stop</i>)			ISO (<i>stop</i>)		
	ρ_1	EXIF	Pred.	ρ_2	EXIF	Pred.	ρ_3	EXIF	Pred.
(a)	4.8	5	5.7	4.6	8	8.6	2.7	7	8.1
(b)			13.8			29.1			-0.8
(c)			4.1			8.5			6.2
(d)			10.4			9.8			7.1
(e)		5	3.5		7	10.6		5	3.4
(f)			8.2			12.6			2.2

4.3.5 Countering Anti-forensics Threat

In this section, we investigate the capability of our approach in resisting the anti-forensics threat lodged by the sophisticated anti-forensics person. With the knowledge of the proposed method, our task is to see if an anti-forensics person can restore the correlation between the images and the EXIF headers by simply recalibrating the EXIF headers on the manipulated images. In the case that the anti-forensics person could make all three constraints corresponding to the three EXIF header features satisfied, he/she would succeed in surpassing our system with the manipulated image.

Assuming the anti-forensics person knows exactly our features selected and their weights for each parameter, the anti-forensics person can attempt to fool the EXIF-Image model by recalibrating either the EXIF parameters or the manipulated image noise features. Although both ways are possible, it is difficult to make the manipulated image noise features properly match with the three EXIF parameters at the same time in reality. In this case, we suppose that the anti-forensics person recalibrate aperture, exposure time and ISO speed rating in the EXIF headers. The anti-forensics person first extracts the statistical image noise features and then estimates the EXIF header feature $\tilde{Y}_j$ by multiplying the weights with the statistical image noise features. The estimated EXIF feature $\tilde{Y}_j$ is a non-discrete value. The anti-forensics person

then rounds off each non-discrete value to the nearest discrete stop according to the standard setting of digital camera system. With this conversion, the discrete EXIF header feature value would be

$$y_j = \tilde{Y}_j + e_j \quad (4.12)$$

where $j = 1, \dots, 3$ and e_j is the round-off error. In order to test the effectiveness of the anti-forensic operation, we randomly select 600 intact images and the corresponding 10800 manipulated images based on the earlier defined six different curves of brightness and contrast adjustment in three different color spaces for the EXIF-Image model. The remaining 600 intact images are manipulated in the same way as before. Suppose that the sophisticated anti-forensics person knows our detection system well and each manipulated image is restored, we perform the same manipulation detection technique proposed. Our experimental result shows that 94.5% of the manipulated images with recalibrated EXIF headers are still correctly detected as manipulated based on the combination rule in Eq. (4.9) and Eq. (4.10). Our high detection accuracy for these recalibrated images owes to the practical difficulty of keeping the modified EXIF values in the normal range and meanwhile introducing the least quantization errors. Frequently, image manipulation would result in the predicted EXIF values beyond the practical range, which enables our proposed EXIF-Image model effectively to resist the anti-forensics threat. Below, we zoom in a common example.

The manipulated image in Figure 4.14(b) is generated from an intact image in Figure 4.14(a). By using the EXIF-Image model for a corresponding EXIF parameter, the new EXIF parameters are estimated as shown in Table 4.8. For instance, Figure 4.14(a) is taken with aperture of 3. We assume that the anti-forensics operation uses the dedicated EXIF-Image model for aperture of 5 to obtain the predicted aperture of 3.95, and then modify the aperture of 4 in Figure 4.14(b) since 4 is the nearest valid aperture stop. Since the aperture of 4 is now in the EXIF header, the anti-forensics person uses the EXIF-Image model for aperture of 4 to predict the new EXIF value to be 7.5. Our detection system would still successfully detect the image as being manipulated.

(a)

(b)

Figure 4.14: Photo (a) with f-number = 2.8, exposure time = $\frac{1}{125}$, ISO = 100; (b) with f-number = 4.0, exposure time = $\frac{1}{1000}$, ISO = 800.

What we have shown here is that defeating our system would not be a trivial task for a sophisticated anti-forensics person, e.g. through simply recalibrating a few EXIF values. The round-off errors are difficult to avoid even if the anti-forensics person wants to restore the EXIF-Image correlation for the manipulated image because legitimate EXIF features consist of only a discrete set of values.

Similar to attacking other security systems, a sophisticated anti-forensics person

Table 4.8: EXIF parameter estimation for the photos in Figure 4.14

Photo	Aperture (<i>stop</i>)		Shutter (<i>stop</i>)		ISO (<i>stop</i>)	
	EXIF	Predicted	EXIF	Predicted	EXIF	Predicted
(a)	3	2.7	7	6.4	5	4.6
(b)	4	7.5	10	18.7	8	15.0

can find many ways to attack our detection system. Besides tampering the EXIF header parameters, it is possible to change the image noise values for the proper EXIF parameters to manipulate the image.

Specifically, the anti-forensics person uses the Olympus camera to take two images of the same scenery with different camera settings as shown in Figure 4.15. The two intact images in Figure 4.15(a) and (b) appear to be captured in the daytime and the night time, respectively. By applying our EXIF-Image model from the Olympus camera to these two images, they are both correctly determined as the intact images. Suppose that the anti-forensics person possesses only the image in Figure 4.15(a) as the original and he wants to generate another image that is similar to Figure 4.15(b) from (a). If the new image can be generated exactly as that in Figure 4.15(b), the anti-forensics person would defeat our manipulation detection framework. However, since the anti-forensics person does not have the exact image in Figure 4.15(b), he can only rely on some prior knowledge to approximate the image in Figure 4.15(b) from (a). This prior knowledge can be a mapping curve of pixel values.

To generate the mapping curve, the anti-forensics person can choose the regions highlighted in previous two images in Figure 4.16(a) and (b). The highlighted areas are chosen because of its large pixel value range. Based on pixel values in these two regions, the anti-forensics person can find a mapping of pixel values in the two regions. Figure 4.17 plots the corresponding pair of pixel values from Figure 4.16(a) and (b), respectively. Through curve fitting, we obtain the pixel-value mapping curve below and also highlighted in Figure 4.17, which gives the least root mean square mapping errors.

$$G(g) = 0.059e^{1.463g} \quad (4.13)$$

(a)

(b)

Figure 4.15: Images are captured of the same scenery by an Olympus E500 camera with different settings of f-number. (a) f-number = 2.8. (b) f-number = 8. Exposure time and ISO are fixed at $\frac{1}{125}$ second and 100.

where g is a normalized pixel value of Figure 4.16(a), $0 \leq g \leq 1$. This mapping curve can serve as the prior knowledge found by the anti-forensics person to manipulate Figure 4.16(a) either in RGB color channels or in the luminance channel to have an image similar to the resultant image in Figure 4.18. If we apply our method to detect the image in Figure 4.18, we can confidently determine this image as a manipulated

(a)

(b)

Figure 4.16: The block areas are chosen from the green color channel of the captured images.

image.

Above all, although it is possible for the anti-forensics person to change either the EXIF parameters or the noise value to perform anti-forensics operation, it's hard to implement in reality.

Figure 4.17: Fitting the mapping curve from the block areas of Figure 4.16(a-b).

Figure 4.18: The manipulated image resulted from Figure 4.16(a) by the fitting mapping curve.

4.4 Summary

In this chapter, we proposed a novel method to correlate statistical image noise features with three selected EXIF header features, which are closely related with

camera shot settings. In computation of these noise features, our method uniquely excluded the sharp image area to minimize the adverse impact caused by different image contents on our features. Also through incorporating the second-order image noise features and sequential floating forward selection, we derived a set of noise features that are correlated with a target EXIF feature and at the same time, the correlation is fragile to image manipulations. By formulating each EXIF feature as a weighted average of its selected noise features, we employed a least squares solution to solve the regression weights from the intact images. These weights allow us estimating the target EXIF feature parameters from the selected noise features. Experimentally, we find that the numerical difference can serve as an excellent indicator to detect the presence of different image brightness and contrast adjustment. Comparisons show that our algorithm not only works well to detect the contrast manipulations but also works well to detect the pure brightness adjustment. Our model also demonstrates a consistent capability for detecting brightness and contrast manipulations without knowing the camera brand/model. As brightness and contrast adjustment often forms an integral part of image forgery creation, several examples show the feasibility of using our model in detection of the real-world image forgeries. Moreover, we show that it is difficult to defeat our system by simply recalibrating the three EXIF values on manipulated images as it is hard to meet the three EXIF-image constraints associated with aperture, shutter speed and ISO, simultaneously.

Chapter 5

EXIF-White Balance Recognition for Image Forensics Analysis

Aperture, shutter speed, and ISO in the EXIF header has been developed for passive forensics. In order to explore rich information recorded in the EXIF header for forensics analysis, we propose a novel approach for image forensics analysis by recognizing different white balance levels in the EXIF header. We first extract image quality metrics features between each two combination of one original image and twelve re-balanced images. By regularizing the eigen spectrum of image quality metrics, the compact set of image eigen features are selected for recognizing different EXIF-white balance levels by SVM classifier. Image manipulation like copy-and-paste operation can affect these image eigen features and lead to a wrong white balance level. By using the EXIF-white balance parameter as a manipulator indicator, we achieve the good and reliable performance in detecting malicious operation, e.g. copy-and-paste operation followed by the high compression or downsampling. Furthermore, our proposed method has the ability to detect the manipulated images which are operated by different white balance post-processings. Several detection examples suggest that our model can be applied in detecting real-world forgeries.

5.1 Introduction

Conventionally, copy-and-paste is defined as such an operation, where a part of a digital image is copied and pasted into a different part of the same image or the different image. Nowadays, in order to make the manipulated image acceptable by the human eyes and weaken the trace of the artifacts introduced by the manipulations, many post-processing operations are performed after copy-and-paste, such as high compression or downsampling. Since the manipulated images can deceive the people from the truth, this complex image tampering as a malicious operation becomes a more difficult and challenging issue for image forensics analysis.

In this chapter, we propose a new approach for image forensics analysis by recognizing white balance levels in the EXIF [3] header, which correlates image quality metrics (IQM) features with EXIF-white balance through image eigenfeature regularization. In the scenario of the complex image tampering detection, for example, when the image is subject to copy-and-paste operation followed by the high compression or downsampling, the estimated white balance level from the image will be different with the one recorded in the EXIF header. To the best of our knowledge, our method is the first to establish a link between the image and white balance parameter in the EXIF header for such a complex image manipulation detection.

Prior works on copy-and-paste detection focus on the operation with low compression, where copy-and-paste is considered that the local interested area is copied and pasted into the same image or different images. Lucas *et al.* [28] proposed an approach by learning the photo response non-uniformity (PRNU) sensor pattern noise to localize the forged region. Specifically, the local PRNU patterns are estimated for one testing photo, and subsequently correlated with the learned reference PRNU patterns by using shapes and sizes of various sliding blocks. The results show that the tampered region of interest is automatically detected and relatively reliable identification is achieved at a JPEG quality factor of 70. By further improving the PRNU model, Chen *et al.* [45] investigated on integrity verification of the images. A probabilistic

score is calculated for exposing the forgery by measuring the correlation statistics of each pixel in a sliding block size of 128×128 . For JPEG quality factor of 75, the integrity verification results based on 345 cut-and-paste forged Canon G2 images, where the forgery area is limited to 228-512 pixels, shows that in 73% of the forgeries, at least 2/3 of the forged area is correctly identified, while in 21% of all the cases, more than 20% of the falsely detected pixels are available. Cao and Kot [93] utilized the demosaicing regularity to detect image manipulation. At a typical quality factor of 80, 83% test accuracy based on 200 SFFS-selected features still suggests reliable identification performance. In [44], He *et al.* determined the doctored blocks by detecting double-quantization effect when a JPEG image is recompressed by a high quality factor. The discrete cosine transform coefficients of each block are computed as the probability of being doctored, which is subsequently used to visually detect the image forged area by the forensics analyst. However, all the works [28, 44, 45, 93] above only report the results for copy-and-paste followed by relatively low compression. Amerini *et al.* [61] proposed an approach by using scale invariant features transform (SIFT) to detect the forged image which is subject to copy-move attack, i.e. copying the local interested area and pasting it into the same image. With the diverse JPEG quality factors (75, 50, 40 and 20) for all the images or copied patch, the results show that all TP and FP rates reach 87.15-100% and 10.46-12.07% respectively. Although this work can detect the forged image with good performance, it's worth noting that the forged image is generated by copying the local interested area and pasting it into the same image.

In this chapter, we develop a novel model through image eigenfeature regularization for each white balance level in the EXIF header, which demonstrates the good performance in detecting the copy-and-paste operation followed by the high compression or downsampling. Our work in this chapter has four main contributions: (1) We propose an approach of image manipulation detection by exploiting EXIF-white balance information which is ignored by previous techniques. (2) Our proposed approach has the ability to recognize different white balance levels applicable for image

manipulation detection. (3) Our proposed approach can detect the complex image tampering, i.e. copy-and-paste followed by the high compression or downsampling, with good performance. (4) Our proposed approach has the ability to detect the manipulated image, which is operated by different types of white balance algorithms.

This chapter is organized as follows. Section 5.2 introduces the potential correlation between the image and the white balance parameter in the EXIF header. Section 5.3 details the feature extraction and regularization of image quality metrics for recognizing different white balance levels, and the manipulated images discrimination from the intact images. In Section 5.4, a set of experiments demonstrate the effectiveness of the proposed EXIF-white balance recognition for image manipulation detection. Section 5.5 concludes this chapter.

5.2 Background

In this chapter, we are particularly interested in white balance among various EXIF tags of camera settings which record the picture-taking surrounding conditions. As a commonly used tag, white balance is provided by the EXIF header in a JPEG image. Meanwhile, white balance as a comprehensive post-processing operation exists in the image acquisition process. In an ideal case, white balance is applied by all digital cameras to correct images from the color of the light source, e.g. to ensure consistent color reproductions for images or to remove unnatural color looking casts. However, due to a difficult challenge to digital photography, the output color from a camera often differs from how it appears to the eyes of the photographer that takes the photo. As an example, Figure 5.1(a-d) show four photos captured of a plain white piece of A4 printer paper indoor with the fluorescent strip light tubes under different white balance settings. We observe that although the lighting condition and the other camera settings are the same, different white balance levels affect the photo appearance in different phases. Furthermore, we are inspired by the investigation that a digital image would not change much compared with the re-balanced image

Figure 5.1: Photos are taken of a plain white piece of A4 printer paper indoor on the board under the white fluorescent strip light tubes by Canon 550D with f-number = 5.6, exposure time = $\frac{1}{200}$, and ISO = 6400.

when the same auto white balance algorithm is performed on the image twice in [140]. Although we do not know the specific white balance algorithm for each white balance level used in the commercial digital cameras sold today, we believe that the majority of the digital cameras are designed for adjusting different lighting conditions by applying multiple white balance technologies, and there exists some discrimination among different digital cameras. Based on the investigation above all, we propose an approach for image forensics analysis by recognizing different white balance levels in the EXIF header.

Figure 5.2: Block diagram of the proposed method.

5.3 Proposed Detection Framework

The proposed framework is to recognize EXIF-white balance levels as shown in Figure 5.2, which is detailed in the following sections. The rational is that the intact images taken under the same white balance level from each camera model retain intrinsic statistical consistency since different images captured of a variety of scenes have gone through the same processing pipeline inside camera. While the image undergoes a type or multiple types of manipulations, the intrinsic statistical consistency can be destroyed or the artifacts can be introduced for discovering the given image as the forgery. In the following section, we elaborate our main steps in Figure 5.2.

5.3.1 White Balance Algorithms for Image Quality Metrics

As mentioned earlier, we are inspired by the investigation that a digital image would not change much when the same auto white balance algorithm is performed on the image twice, and the re-balanced image would have different patterns if different auto white balance algorithms are applied on the image [140]. In this chapter, a given image is represented by a set of image quality metrics (IQM) features between one original image of a given camera and twelve re-balanced images by using various

Table 5.1: Overview of different white balance algorithms.

Algorithm	Hypothesis	Description
Gray world	the average reflectance in a scene is achromatic	Diagonal [148] Von Kries Bradford Sharp CMCCAT2000 [149] XYZ model [150]
Shades of gray	the pth-Minkoweky norm of a scene is achromatic	[151]
Gray edge	the pth-Minkoweky norm of the image derivative in a scene is achromatic	differentiation order 1 differentiation order 2 [152]
White patch	the maximum reflectance in a scene is achromatic	with percentage of white set to be $\frac{1}{255}$ with percentage of white set to be 0.01 max-RGB with smoothing

white balance algorithms, rather than finding one specific white balance algorithm used inside the source camera.

So far a considerable amount of literatures [148–152] on white balance algorithms have been reported under different assumptions. Since more commercial digital cameras sold today use white balance algorithms under gray-world assumption, we choose more variations of gray world algorithms than white assumption in this chapter. Specifically, we choose $D = 12$ types of the commonly used white balance algorithms as shown in Table 5.1. For instance, the first six types of gray world algorithms are based on the assumption that the average reflectance in a scene is achromatic, and they use six different adaptation methods including Diagonal [148], Von Kries, Bradford, Sharp and CMCCAT2000 [149] and XYZ model [150]. More details can be referred to [148–152].

After applying D different white balance algorithms for a given original color image $\mathbf{A}$ of $M \times N$ size, the corresponding re-balanced images $\hat{\mathbf{A}}$ are generated. Different from the work in [140], we do not only measure the difference between the original image and the re-balanced image, but also catch the difference between each two

Table 5.2: Image quality metrics feature pool.

Scope	Algorithm	Description	Dimension
Minkowsky Metrics	Mean Absolute Error	$MAE(c) = \left\{ \frac{1}{M \times N} \sum_{m=1, n=1}^{M, N} A(m, n, c) - \hat{A}(m, n, c) \right\}$	3
	Mean Square Error (MSE)	$MSE(c) = \left\{ \frac{1}{M \times N} \sum_{m=1, n=1}^{M, N} A(m, n, c) - \hat{A}(m, n, c) ^2 \right\}$	3
	Maximum Difference	$MD(c) = \max\{ A(m, n, c) - \hat{A}(m, n, c) \}$	3
	Normalized MSE	$NMSE(c) = \frac{M \times N \times MSE(c)}{\sum_{m=1}^M \sum_{n=1}^N A^2(m, n, c)}$	3
	Peak Signal to Noise Ratio	$PSNR(c) = 20 \lg \frac{255}{\sqrt{MSE(c)}}$	3
Correlation Metrics	Czekznowski Correlation	$CC = 1 - \frac{2 \times \sum_{m=1, n=1}^{M, N} \sum_{c=1}^3 \min(A(m, n, c), \hat{A}(m, n, c))}{\sum_{m=1, n=1}^{M, N} \sum_{c=1}^3 (A(m, n, c) + \hat{A}(m, n, c))}$	1
	Angle Mean	$AM = 1 - \frac{1}{M \times N} \sum_{m=1, n=1}^{M, N} \frac{2 \langle A(m, n), \hat{A}(i, j) \rangle}{\prod \ A(i, j) \times \ \hat{A}(i, j)\ }$	1
	Structural Content	$SC(c) = \frac{\sum_{m=1, n=1}^{M, N} A(m, n, c)^2}{\sum_{m=1, n=1}^{M, N} \hat{A}(m, n, c)^2}$	3
	Correlation Quality	$CQ(c) = \frac{\sum_{m=1, n=1}^{M, N} A(m, n, c) \hat{A}(m, n, c)}{\sum_{m=1, n=1}^{M, N} A(m, n, c)^2}$	3
	HVS real lab distance HVS similarity weight	First transform the image into HVS mdoel and then compute a similarity measure in discrete wavelet domain	1 1
Spectral Measures	Block Weighted Spectral Distance (max,mean,median)	First extract the weighted metrics for each block in discrete Fourier domain and then use the max, mean, median value as potential feature	3×3

of re-balanced images. In such a way, we can catch more subtle variations between each two combination of one original image and D re-balanced images generated by different white balance algorithms. Totally, $\binom{2}{D+1} = 78$ combinations are obtained from 1 original image and $D = 12$ re-balanced images. We then use IQM features [110, 153, 154] to represent the difference. Specifically, the main concept and procedures of IQM are briefly summarized as shown in Table 5.2, which include Mean Absolute Error, Mean Square Error (MSE), Normalized MSE, Peak-Signal-to-Noise Ratio, Maximum Difference, Czekznowski Correlation, Angle Mean, Structural Content, Correlation Quality, HVS real lab distance, HVS similarity weight, and Block Weighted Spectral Distance (max,mean,median).

Finally, an overall feature vector for a given image contains $L = 34 \times 78 = 2652$ dimensions. This improves our estimation of the correlation between the image quality features and the EXIF-white balance parameter.

5.3.2 Eigen Feature Regularization

The compression and downsampling operations make the IQM features difficult to be directly utilized for EXIF-white balance recognition, especially when the high dimensional features are extracted from a relatively small set of training images with the high compression or downsampling rate. Ideally, it is often desirable to minimize the within-class covariance and maximize the between-class covariance for good classification. However, the compression and downsampling operations would adversely affect IQM features and lead to an increased within-class covariance. In order to improve the reliability, a compact set of discriminant eigen features is derived for image forensics analysis through an eigen feature transformation technique in [155].

A set of $P \times Q$ training images are given, where P denotes the total number of white balance levels, Q denotes the number of sample images for each balance level. $\{\mathbf{x}_{pq} | 1 \leq p \leq P, 1 \leq q \leq Q\}$, $\mathbf{x}_{pq} \in \mathbb{R}^L$, denoted the normalized training feature vectors, where a linear normalization is performed on each feature so that it has zero

mean and unity variance.

Figure 5.3: Eigen spectra of IQM feature set of the training images with QF=20 including three different white balance levels, and the regularized eigen spectra.

We first compute the within-class covariance matrix $\mathbf{S}^{(w)}$ as

$$\mathbf{S}^{(w)} = \frac{1}{PQ} \sum_{p=1}^P \sum_{q=1}^Q (\mathbf{x}_{pq} - \bar{\mathbf{x}}_p)(\mathbf{x}_{pq} - \bar{\mathbf{x}}_p)^T \quad (5.1)$$

where $\bar{\mathbf{x}}_p = \frac{1}{Q} \sum_{q=1}^Q \mathbf{x}_{pq}$ is the mean vector of the p -th white balance level.

The eigen decomposition is then performed by using

$$\mathbf{\Lambda}^{(w)} = \mathbf{\Phi}^{(w)T} \mathbf{S}^{(w)} \mathbf{\Phi}^{(w)} \quad (5.2)$$

where $\mathbf{\Phi}^{(w)} = [\varphi_1^{(w)}, \dots, \varphi_L^{(w)}]$ is the eigenvector matrix of $\mathbf{S}^{(w)}$ and $\mathbf{\Lambda}^{(w)}$ is the diagonal matrix with the corresponding eigen values $\lambda_1^{(w)} \geq \lambda_2^{(w)} \geq \dots \geq \lambda_L^{(w)}$. As an example in Figure 5.3, the eigen spectrum of the IQM feature set of the training images with QF=20 is shown in the log-scale. It consists of three different white balance levels. Since the high dimensional features are extracted from the relatively limited number of training images, especially when training images are operated by the high compression or downsampling operation, the generated eigen values from these training images will

have less generalization capability which causes them less reliable. In order to increase the reliability of the training image set, the eigen spectrum is regularized as [155].

Specifically, the eigen spectrum is categorized into 3 regions, which are “signal”, “noise” and “null”. By choosing several model parameters T , R , α and β according to [155], the regularized eigen value corresponding to the l -th eigenvector is written as

$$\tilde{\lambda}_l^{(w)} = \begin{cases} \lambda_l^{(w)} & \text{if } l < T \\ \frac{\alpha}{l+\beta} & \text{if } M \leq l \leq R \\ \frac{\alpha}{1+R+\beta} & \text{if } R \leq l \leq L \end{cases} \quad (5.3)$$

As shown in Figure 5.3, we can see that the regularized eigen spectra is closer to the eigen spectrum curve in the noise region and the unreliable spectra in the “null” region are replaced by a constant spectra.

The whitening feature transformation is computed by using

$$\mathbf{y}_{pq} = \tilde{\Psi}_L^{(w)T} \mathbf{x}_{pq} \quad (5.4)$$

where the whitening transformation is $\tilde{\Psi}_L^{(w)} = \left[\frac{\varphi_1^{(w)}}{\sqrt{\lambda_1^{(w)}}}, \dots, \frac{\varphi_L^{(w)}}{\sqrt{\lambda_L^{(w)}}} \right]$. Based on the $\mathbf{y}_{pq}$, we compute the total covariance matrix using

$$\mathbf{S}^{(t)} = \frac{1}{PQ} \sum_{p=1}^P \sum_{q=1}^Q (\mathbf{y}_{pq} - \bar{\mathbf{y}}_p)(\mathbf{y}_{pq} - \bar{\mathbf{y}}_p)^T \quad (5.5)$$

where $\bar{\mathbf{y}}_p = \frac{1}{PQ} \sum_{p=1}^P \sum_{q=1}^Q \mathbf{y}_{pq}$ is the global mean vector. Similar with Eq. (5.2), the eigen decomposition is performed on $\mathbf{S}^{(t)}$. Figure 5.4 shows the eigen spectra of $\mathbf{S}^{(t)}$ for the compression operations, which include the original image and the quality factors of 70, 50 and 20, respectively. We can see that by using the whitening transformation in Eq. (5.4), 4 different eigen spectra of $\mathbf{S}^{(t)}$ possess subtle changes.

Furthermore, significant eigen values can be selected to construct a compact subspace for good classification of white balance levels. By using principal component analysis for feature reduction, the compact eigen feature vector is calculated as

$$\mathbf{z}_{pq} = \tilde{\Psi}_E^{(t)T} \mathbf{y}_{pq} = \mathbf{F} \mathbf{x}_{pq} \quad (5.6)$$

Figure 5.4: Eigen spectra and zoomed version of the total covariance matrix after the whitening transformation.

where $\mathbf{z}_{pq} \in \mathbb{R}^E$, $\tilde{\Psi}_E^{(t)} = [\varphi_1^{(t)}, \dots, \varphi_E^{(t)}]$ is the eigenvector matrix of $\mathbf{S}^{(t)}$ corresponding to the E largest eigenvalues, i.e. $E < L$, which is constructed by principal component analysis (PCA). The learned eigen transformation $\mathbf{F} = (\tilde{\Psi}_L^{(w)} \tilde{\Psi}_E^{(t)})^T$.

5.3.3 Image Forensics Analysis

After learning the eigen transformation, support vector machine (SVM) is used for recognizing different white balance levels in the EXIF header. In the training process, we use one versus all strategy to train an SVM classifier for each white balance level, the radial basis function kernel is used to calculate the distance between two image eigen features. In the testing phase, for a testing image, the learned eigen transformation is performed on it. Then the compact set of eigen features is forwarded to each of the trained SVM classifiers to obtain an output score. In order to determine which white balance level the testing image belongs to, the class that generates the highest SVM output score is treated as the recognized white balance level.

After determining the white balance level for the testing image, the final detection is determined as

$$U = \begin{cases} 1 & \text{if } u == b \\ 0 & \text{if } u \neq b \end{cases} \quad (5.7)$$

where u is the SVM recognized white balance level, and b is the white balance level in the EXIF header. $U = 1$ denotes the intact class, and $U = 0$ is for the manipulated class where either the image content or the EXIF header is tampered.

Table 5.3: Key parameters of three different cameras.

Camera model	Image resolution (pixels)	White balance
Nikon D3000	1936×1296	Fluorescent, Tungsten, Sunny/Auto
Canon 550D	2592×1728	Fluorescent, Tungsten, Sunny/Auto
Olympus E500	2560×1920	Fluorescent, Tungsten, Fineweather/Auto

(a) Fluorescent

(b) Tungsten

(c) Sunny/Auto

Figure 5.5: Some photo samples from Canon 550D camera.

5.4 Experiments and Discussion

5.4.1 EXIF-White Balance Recognition on Compressed Images

In this section, we testify the effectiveness of the proposed method for EXIF-white balance recognition based on the compressed images with different quality factors.

Two sets of experiments are conducted. One is to compress the training images and the testing images by the same quality factor value. The other set is more challenging and closer to reality, that is only the original training images are used to determine the compressed testing images with multiple quality factors. More details are discussed as below.

Set 1

We collect 1350 photos in total with each 450 photos from three different camera brands, which are Canon, Olympus and Nikon. For each camera brand, the dataset contains 150 photos from each of 3 commonly used white balance levels of fluorescent, tungsten, and sunny/auto in companion with the digital cameras. Key parameters of the camera dataset are shown in Table 5.3. These photos are randomly taken of various scenes with different camera settings under the surrounding lighting conditions. Some samples of the dataset are shown in Figure 5.5.

In our experiments, the MatLab function *imwrite* was used to compress the original JPEG images. This function allows the JPEG Quality Factor (QF) to be within the range of $[0,100]$, where 0 denotes an image has lower quality and higher compression rate, and 100 denotes an image has higher quality and lower compression rate. Specifically, 300 JPEG images are randomly selected from each camera, where 100 images from one of three white balance levels. SVM classifier is then trained for each class using one versus all strategy. The remaining images are used for testing.

Three classes of white balance levels are respectively class 1 of sunny/auto (or fineweather/auto for Olympus), class 2 of fluorescent, and class 3 of tungsten. When the eigen decomposition is performed on the total covariance, 2652 eigen values are obtained in descending order. In order to find the significant eigen features for forensics analysis, we use SVM score as the criterion to select a compact feature subset. As an example in Figure 5.6(a), we plot SVM scores against the number of selected eigen features for the original training images. It shows that the SVM score increases

(a)

(b)

Figure 5.6: SVM scores against the number of selected features for (a) the original and (b) compressed training images with QF=20.

to a maximum and then decreases gradually when the number of selected features increases. When 40 features are selected, SVM score achieves the maximum. We then utilize a compact set of 40 selected eigen features for learning SVM model. Similarly, Figure 5.6(b) shows that 47 eigen features are selected from the compressed training images with quality factor of 20.

After applying the learned SVM model for testing, Table 5.4 shows a performance

Table 5.4: The performance comparison for the original and compressed images from different camera sources.

Train (QF)	Test (QF)	Camera brand	Class 1 TP (%)	Class 2 TP (%)	Class 3 TP (%)	Class 1 FP (%)	Class 2 FP (%)	Class 3 FP (%)	Average (%)
Ori.	Ori.	Nikon	100.0	86.0	90.0	3.0	5.0	4.0	92.0
		Canon	94.0	88.0	86.0	6.0	9.0	1.0	89.3
		Olympus	82.0	86.0	98.0	7.0	9.0	1.0	88.7
70	70	Nikon	100.0	84.0	90.0	4.0	4.0	5.0	91.3
		Canon	96.0	90.0	80.0	5.0	11.0	1.0	88.7
		Olympus	82.0	84.0	98.0	9.0	9.0	0.0	88.0
50	50	Nikon	100.0	82.0	88.0	6.0	4.0	5.0	90.0
		Canon	90.0	86.0	86.0	6.0	11.0	2.0	87.3
		Olympus	82.0	82.0	98.0	9.0	9.0	1.0	87.3
20	20	Nikon	100.0	84.0	86.0	4.0	6.0	5.0	90.0
		Canon	90.0	88.0	82.0	5.0	11.0	4.0	86.7
		Olympus	80.0	82.0	98.0	1.0	9.0	1.0	86.7

comparison of three different white balance levels recognition in the original and compressed images from three cameras in terms of TP (True Positive), FP (False Positive) and average rate, where TP is the rate of the correctly classified testing images over all the testing images for the given white balance level, FP is the rate of the wrongly classified testing images over all the testing images for the given white balance level, and the average rate is averaged the TP rates among all three classes. For instance, we find that for the Nikon original images, the TP rates of 100%, 86.0%, and 90.0% for sunny/auto, fluorescent and tungsten are achieved while the FP rates of 3.0%, 5.0% and 4.0% are achieved for sunny/auto, fluorescent and tungsten, respectively. By averaging all TP rates of three classes, we achieve 92.0% average rate. For the Nikon compression images with QF of 70, 50 and 20, the average rates are 91.3%, 90.0% and 90.0%, respectively. Similarly, we have conducted the experiments for Canon and Olympus cameras with more than 86.7% average rates achieved. By observing the experimental result, our method can be reliable to distinguish different white balance levels even when the images are subject to the high compression operation.

Set 2

We evaluate the framework of EXIF-white balance recognition in a more challenging and realistic situation, due to the difficulty in learning the prior knowledge of the quality factor of the compression image in practice. Hence, our proposed framework is urgently needed to distinguish different white balance levels by only using the original images for training. The same experimental procedure is conducted based on the same dataset, while only the learned SVM model of original images is applied for testing the compression images with different quality factors.

Table 5.5: The performance comparison for the compressed images from different camera sources.

Train	Test (QF)	Camera brand	Class 1 TP (%)	Class 2 TP (%)	Class 3 TP (%)	Class 1 FP (%)	Class 2 FP (%)	Class 3 FP (%)	Average (%)
Ori.	70	Nikon	100.0	82.0	88.0	3.0	6.0	6.0	90.0
		Canon	92.0	88.0	80.0	5.0	13.0	2.0	86.7
		Olympus	80.0	82.0	98.0	1.0	9.0	1.0	86.7
	50	Nikon	100.0	82.0	86.0	3.0	6.0	7.0	89.3
		Canon	94.0	86.0	80.0	6.0	12.0	2.0	86.7
		Olympus	84.0	86.0	98.0	8.0	7.0	1.0	89.3
	20	Nikon	100.0	80.0	86.0	3.0	6.0	8.0	88.7
		Canon	88.0	86.0	84.0	5.0	12.0	4.0	86.0
		Olympus	84.0	82.0	98.0	1.0	7.0	1.0	88.0

Table 5.5 shows a performance comparison for the compressed images from three cameras, which are compressed by QFs of 70, 50 and 20 respectively. As shown in Table 5.5, for testing the Nikon compressed images with QF of 70, the TP rates of 100.0%, 82.0%, and 88.0% are achieved for sunny/auto, fluorescent and Tungsten while the FP rates are 3.0%, 6.0% and 6.0% for sunny/auto, fluorescent and tungsten, respectively. By averaging all TP rates for three classes, 90.0% average rate is achieved. For the Nikon compression images with QFs of 50 and 20, the average rates are 89.3% and 88.7%, respectively. Similarly, we have conducted the experiments for the compressed images from Canon and Olympus cameras, and more than 86.0% rates on average are achieved. The consistently good performance for the com-

pressed images with three different quality factors demonstrates that the proposed method can be reliable for EXIF-white balance recognition even when the images are undergoing high compression operation with QF of 20.

Table 5.6: The performance comparison for the resized images from different came sources.

Train	Test (Resized)	Camera brand	Class 1 TP (%)	Class 2 TP (%)	Class 3 TP (%)	Class 1 FP (%)	Class 2 FP (%)	Class 3 FP (%)	Average (%)
Ori.	$\frac{1}{2}$	Nikon	98.0	88.0	90.0	3.0	5.0	5.0	92.0
		Canon	92.0	88.0	82.0	5.0	13.0	2.0	87.3
		Olympus	84.0	86.0	98.0	1.0	7.0	1.0	89.3
	$\frac{1}{4}$	Nikon	98.0	82.0	88.0	3.0	6.0	7.0	90.0
		Canon	94.0	86.0	82.0	6.0	9.0	2.0	87.3
		Olympus	84.0	86.0	96.0	5.0	6.0	1.0	88.7
	$\frac{1}{8}$	Nikon	96.0	82.0	86.0	4.0	6.0	6.0	88.0
		Canon	88.0	86.0	84.0	5.0	8.0	4.0	86.0
		Olympus	84.0	84.0	98.0	3.0	7.0	1.0	88.7

5.4.2 Determining EXIF-White Balance Levels on Resized Images

Some forensics clues are fragile for the image which is resized by downsampling operation, such as demosaicing regularity. That is because that downsampling operation deteriorates the uniqueness of detected demosaicing regularity since demosaicing regularity contains rich correspondence among neighboring color samples. We here investigate the performance of the proposed framework for the resized images in a challenging and realistic situation. Specifically, 450 intact images from the same dataset as before are used in the experiments. 300 intact images are randomly selected, with every 100 images taken from three different white balance levels. Then 300 randomly selected intact images are used for training SVM model and determining the compact subset of eigen features, the remaining images altered by multiple downsampling operations with $\frac{1}{2}$, $\frac{1}{4}$ and $\frac{1}{8}$ are for testing. By applying the learned SVM model through the eigen features regularization, the experimental results are obtained as shown in Table 5.6.

Table 5.6 shows the performance comparison of the resized images from three cameras for EXIF-white balance recognition in terms of TP, FP and average rates. For instance, we find that for the Nikon resized testing images by $\frac{1}{2}$ downsampling operation, the TP rates of 98.0%, 88.0% and 90.0% are achieved for sunny/auto, fluorescent and tungsten while the FP rates of 3.0%, 5.0% and 5.0% are achieved for sunny/auto, fluorescent and tungsten, respectively. By averaging all three classes TP rates, we achieve 92.0% average rate. For the Nikon resized images by downsampling operations with $\frac{1}{4}$ and $\frac{1}{8}$, the average rates are 90.0% and 88.0%, respectively. Similarly, we have conducted the experiments for Canon and Olympus resized images by downsampling operations with $\frac{1}{2}$, $\frac{1}{4}$ and $\frac{1}{8}$, average rates of higher than 86.0% are achieved. By observing the experimental results, we find that our method has ability to reliably distinguish different white balance levels even when the testing images are subject to the downsampling operation.

5.4.3 Detection of Forgery Photos

Nowadays, the image editing tool is rapidly developed and easily applied since it covers a variety of function for image manipulation. White balance operation as a common form of image manipulation, is found in Photoshop software. White balance operation can improve the overall perception of an image, especially while the lighting condition and surrounding of the image are changed differently. Hence, it can fool others in deceiving from the truth. For example in Figure 5.7, images (a-b) contain the same scenery but different time appearances. By observing these two images, it appears that (a) is captured in the sunrise or sunset moment and (b) is captured in the daytime. Visually, it is difficult for one to figure out which of these two images is manipulated. While applying our proposed method to these two images, we confidently differentiate the manipulated image from the intact image. We first determine the white balance level of image (a) and compare the estimated white balance level with the corresponding EXIF-white balance. As shown in Table 5.7, the predicted white balance level of image (a) is sunny/auto. Compared with the white

Figure 5.7: Manipulated images (b) and (d) are generated from intact image (a) and (c) by white balance post-processing.

balance level of auto in the EXIF header, image (a) is determined as intact. Image (b) is detected as manipulated, since the predicted white balance level is fluorescent and the EXIF-white balance level is auto. In another similar case, images (c-d) appear different but contain the same scene. By applying the proposed method, the comparison between the predicted white balance level and the EXIF-white balance level is used for detecting images (c-d). Finally, images (c) and (d) are correctly determined as intact and manipulated respectively.

In addition, it is possible that white balance operation as a post-processing is in company with copy-and-paste in order to make the manipulated image more acceptable by the human eyes. For example, the manipulated image (c) in Figure 5.8 is generated by first performing copy-and-paste operation in Photoshop for intact images (a-b) together followed by white balance post-processing. In reality, it is diffi-

(a)

(b)

(c)

Figure 5.8: Manipulated image (c) is generated from intact images (a-b) by copy-and-paste followed by white balance post-processing.

cult to discern the manipulated image directly. After applying the proposed method, images (a-b) and (c) in Figure 5.8 are correctly determined as the intact and the manipulated respectively.

Compression and downsampling are often used as a part of malicious image content

Image (a)

Image (b)

Image (c)

Image (d) of QF=70

Image (e) of QF=50

Image (f) of QF=20

Image (g) of $\frac{1}{2}$ resized

Image (h) of $\frac{1}{4}$ resized

Image (i) of $\frac{1}{8}$ resized

Figure 5.9: Manipulated images (d-f) are generated from intact images (a-c) by copy-and-paste followed by compression operation with QF of 70, 50 and 20. Manipulated images (g-i) are created from intact images (a-c) by copy-and-paste followed by down-sampling of $\frac{1}{2}$, $\frac{1}{4}$ and $\frac{1}{8}$.

alternation, e.g. copy-and-paste. When compression and downsampling operations are further used for the manipulated image, some trace can be undermined. For example, three manipulated images (d-f) in Figure 5.9 are created by first operating copy-and-paste in Photoshop for intact images (a-c) together followed by the compression with quality factor of 70, 50 and 20. Similarly, the manipulated images (g-i) are generated by first operating copy-and-paste for intact images (a-c) then followed by the downsampling with $\frac{1}{2}$, $\frac{1}{4}$ and $\frac{1}{8}$. By observing (d-i), it is difficult to recognize the manipulated images using human eyes. However, by using our detection model, we compare the predicted white balance level of the image with the white balance level in the EXIF header. The detection results reliably differentiate that images in (a-c) are intact and images in (d-i) are manipulated.

Table 5.7: EXIF white balance prediction for the images in Figure 5.7-5.9.

Photo Index	WB in EXIF	Predicted WB	Decision
5.7(a)	Auto	Sunny/Auto	Auto
5.7(b)	Auto	Fluorescent	×
5.7(c)	Auto	Sunny/Auto	Auto
5.7(d)	Auto	Fluorescent	×
5.8(a)	Tungsten	Tungsten	Tungsten
5.8(b)	Auto	Sunny/Auto	Auto
5.8(c)	Tungsten	Fluorescent	×
5.9(a)	Sunny	Sunny/Auto	Sunny
5.9(b)	Fluorescent	Fluorescent	Fluorescent
5.9(c)	Tungsten	Tungsten	Tungsten
5.9(d)	Sunny	Fluorescent	×
5.9(e)	Sunny	Fluorescent	×
5.9(f)	Sunny	Fluorescent	×
5.9(g)	Sunny	Fluorescent	×
5.9(h)	Sunny	Fluorescent	×
5.9(i)	Sunny	Fluorescent	×

5.4.4 Investigation of Auto and Sunny White Balance Levels

In our earlier discussion, we combine auto and sunny (or fineweather) as one white balance level. Since these two isolated white balance options are available in the commercial digital cameras, we study the effectiveness of the proposed method for distinguishing images from white balance of auto to white balance of sunny. As shown in Table 5.8, 89.3% average rate and 85.3% average rate are achieved when auto and sunny are considered as an isolated white balance option for classification. When auto and sunny are considered as one class, the average rate is 88.7%.

Table 5.8: The performance comparison for the original images from Canon camera.

Three classes of EXIF-WB values	Class 1 TP (%)	Class 2 TP (%)	Class 3 TP (%)	Class 1 FP (%)	Class 2 FP (%)	Class 3 FP (%)	Average (%)
Auto vs. Fluorescent vs. Tungsten	96.0	88.0	84.0	4.0	2.0	1.0	89.3
Sunny vs. Fluorescent vs. Tungsten	88.0	86.0	82.0	5.0	2.0	1.0	85.3
Sunny/Auto vs. Fluorescent vs. Tungsten	92.0	86.0	88.0	5.0	5.0	1.0	88.7

In order to study the white balance options of auto and sunny, four images as shown in Figure 5.10 are taken under different lighting conditions. Figure 5.10(a-b) are captured outdoor and Figure 5.10(c-d) are captured indoor. By observing these four images (a-d), we find that although images (a-b) and (c-d) are captured of the same scene outdoor or indoor with different white balance options, they almost look similar. Moreover, it is unfortunate that the specific white balance algorithms inside cameras are not exposed. All of these reasons make the EXIF-white balance recognition of auto and sunny difficult. However, in order to deceive the others from the truth, it is possible that the images taken with different white balance options and appeared more different has more opportunities to be chosen for image manipulation.

Figure 5.10: Images (a-b) are taken outdoor with auto and sunny white balance respectively. Images (c-d) are taken indoor with auto and sunny white balance respectively.

5.4.5 Anti-forensics Threat Discussion

In theory, it is possible that white balance value in the EXIF header is not authentic. In other words, the proposed method faces the anti-forensics threat, i.e. EXIF-white balance value of the manipulated image is deliberately edited by the attacker. In such a case, the proposed method will take the risk to determine the manipulated image as the authentic one. As the anti-forensics threat is a research topic by itself, we do not discuss it so deep in this thesis in order to stay within the main focus of the thesis.

5.5 Summary

In this chapter, we proposed a novel method to correlate IQM features with EXIF white balance parameter through eigen feature regularization. In computation of IQM features, our method extracts the difference between each two combination of one original image and twelve re-balanced images to catch more subtle variations between the original image and re-balanced images. Through the eigen feature regularization and principal component analysis, a compact set of image features are derived which are correlated with the white balance level in the EXIF. When image manipulation is performed on the image, image statistical consistency is destroyed. Experimentally, we find that the EXIF white balance can serve as a good indicator to detect image manipulation. When the images are subject to compression operation, more than 86% average rates are achieved, even for the quality factor of 20. Moreover, the experimental results show that the proposed method has ability to distinguish three different white balance levels for the resized images by downsampling of $\frac{1}{2}$, $\frac{1}{4}$ and $\frac{1}{8}$. Several detection examples suggest that our method can be applied in detecting forgery photos, where the image is first operated by copy-and-paste then followed by high compression, downsampling or white balance post-processing.

Chapter 6

Conclusions and Future Works

6.1 Conclusions

In this thesis, we exploited several new evidences from the EXIF header for image forensics purposes. Specifically, the relationship between the image and the corresponding EXIF header is modeled for detecting the manipulated images. To the best of our knowledge, our method is among the first to establish a link between the image and its EXIF header information. The rationale is that the numerical differences between the actual EXIF features and their corresponding estimated EXIF features from the image features can serve as an excellent indicator to determine whether an image represents the original camera recording or it has gone through several types of operations. In order to model the link between the image and the corresponding EXIF header, we developed several models to correlate the image features with the commonly used EXIF header features. A summary of our proposed method is described as follows:

Firstly, the novel evidence is exploited from the EXIF header for image forensics analysis in Chapter 3. The EXIF header feature set is represented by aperture value, shutter speed value, ISO speed rating value, brightness value, and exposure value, respectively. These five items are related to the camera settings. As we know, the camera settings affect the appearance of the image content. Hence, these five

items represent the EXIF header features, which are correlated with the image statistical noise features in the linear regression algorithm. The experimental results demonstrate that the novel evidence is a promising tool for forensics tasks.

Secondly, the proposed manipulation approach in Chapter 4 achieves good performance for detecting brightness and contrast adjustment. The proposed method models the EXIF-Image correlation in the non-linear regression algorithm in order to cater for the nonlinearity of the underlying correlation due to various digital processing operations of a camera system. Specifically, image statistical noise features are extracted from the non-sharp area in the image using the de-noising algorithms. The EXIF header features are refined as aperture, shutter speed and ISO. By applying the EXIF-Image correlation for image manipulation detection, the experimental results show the effectiveness of the proposed method.

Finally, new evidence can be found from the EXIF header for image manipulation detection. The proposed method correlates image quality metrics with EXIF white balance parameter through eigen feature regularization. In computation of IQM features, our method extracts the difference between the original image and each one from the twelve re-balanced images to catch more subtle variations between the original image and re-balanced image. Through the eigen feature regularization and principal component analysis, a compact set of image features are derived which are correlated with the white balance level in the EXIF. When image manipulation is performed on the image, image statistical consistency is destroyed. Experimentally, we find that the EXIF white balance can serve as a good indicator to detect image manipulation. The results are promising.

In pace with seeking good intrinsic correlation for image manipulation detection, this thesis explored a new possibility to model the underlying link between the image and its metadata entries for reliable forensics analysis.

6.2 Future Works

Other than what we have studied in this thesis, many other forms of correlations exist between the image and the corresponding EXIF header which provides rich shot-related information. In the future, there still exists some improvement space to model the correlation between image features and corresponding EXIF header for forensics purposes. Below, several possible research directions are indicated in Figure 6.1.

Figure 6.1: Framework for future work

1. Improving The Correlation between IQM Features and EXIF-White Balance.

The correlation between IQM features and white balance has been proposed in this thesis. However, there is still some room to improve the proposed correlation in order to recognize the images from auto and sunny since these two white balance levels

still have possibilities to be used by the professional photographer. Some challenging issues, such as countering the anti-forensics threat will need to be further investigated.

2. Modeling The Correlation between The Image Blur Features and EXIF-Focal Length

The link between image defocus blur feature is known to be closely related with focal length in the EXIF header. Defocus blur is a type of natural blur. It exists due to the limitation of the lens system. Suppose that the image is tampered by copy-move, splicing, etc. Another type of blur in digital images is called artificial blur, which is incurred by deliberate manipulation. In this case, learning the correlation between the image blur features and EXIF-focal length can be used to detect the tampered images.

3. Recovering The Part of The EXIF Header Information.

Based on all kinds of links between image feature and the corresponding EXIF header features, we will recover the EXIF corresponding to the image. As we know, the EXIF headers may be erased deliberately or lost accidentally. According to the links we established between the image statical noise features and the EXIF header, some parts of the EXIF header information can be recovered, such as camera shot settings. The recovered EXIF can be used for image retrieval purposes.

Author's Publications

Journal Papers

Jiayuan Fan, Hong Cao, and Alex C. Kot, “Estimating EXIF Parameters Based on Noise Features for Image Manipulation Detection”, *IEEE Transactions on Information Forensics and Security*, vol8(4), pp. 608-618, 2013

Jiayuan Fan and Alex C. Kot, “EXIF-White Balance Recognition for Image Forensics Analysis”, *to be submitted to an IEEE Journal*, 2014

Conference Papers

Jiayuan Fan, Alex C. Kot, Hong Cao and Farook Sattar, “Modeling the EXIF-Image correlation for image manipulation detection”, *The International Conference on Image Processing (ICIP)*, pp. 1945-1948, 2011.

Khosro Bahrami, Alex C. Kot, Jiayuan Fan, “A novel approach for partial blur detection and segmentation”, *IEEE International Conference on Multimedia and Expo (ICME)*, pp. 1-6, 2013

Khosro Bahrami, Alex C. Kot, Jiayuan Fan, “Splicing Detection in Out-of-Focus Blurred Images”, *The IEEE International Workshop on Information Forensics and Security (WIFS)*, 2013

Bibliography

- [1] G. Murano, “10 most famous doctored photos.” http://www.oddee.com/item_96803.aspx.
- [2] Camera and I. P. Association, “Exif print.” http://www.cipa.jp/exifprint/contents_e/01exif1_e.html, September 2003.
- [3] T. S. C. on AV & IT Storage Systems and Equipment, “Exchangeable image file format for digital still cameras: Exif version 2.2,” Tech. Rep. JEIDA CP-3451, April 2002.
- [4] Mohylek, “Diaphragm giving a big (f/2.8) and a small (f/16) aperture in the camera lens.” <http://en.wikipedia.org/wiki/File:Aperures.jpg>, August 2006.
- [5] H. Farid, “Photo tampering throughout history: an overview of some of the more notable instances of photo manipulation in history.” <http://www.fourandsix.com/photo-tampering-history/>.
- [6] J. Tesic, “Metadata practices for consumer photos,” *IEEE MultiMedia*, vol. 12, no. 3, pp. 86–92, 2005.
- [7] I. Avcibas, S. Bayram, N. D. Memon, M. Ramkumar, and B. Sankur, “A classifier design for detecting image manipulations,” in *Proc. of International Conference on Image Processing*, pp. 2645–2648, 2004.

- [8] A. C. Popescu and H. Farid, “Statistical tools for digital forensics,” in *In 6th International Workshop on Information Hiding*, pp. 128–147, Springer-Verlag, Berlin-Heidelberg, 2004.
- [9] S. Bayram, I. Avcibas, B. Sankur, and N. D. Memon, “Image manipulation detection,” *Journal Electronic Imaging*, vol. 15, no. 4, p. 041102, 2006.
- [10] H. Farid, “Exposing digital forgeries in scientific images,” in *ACM Multimedia and Security Workshop*, pp. 29–36, 2006.
- [11] A. Swaminathan, M. Wu, and K. J. R. Liu, “Image tampering identification using blind deconvolution,” in *Proc. of International Conference on Image Processing*, pp. 2309–2312, 2006.
- [12] Y. Sutcu, B. Coskun, H. T. Sencar, and N. D. Memon, “Tamper detection based on regularity of wavelet transform coefficients,” in *Proc. of International Conference on Image Processing*, pp. 397–400, 2007.
- [13] E. Kee and H. Farid, “Digital image authentication from thumbnails,” in *Media Forensics and Security*, p. 75410, 2010.
- [14] J. F. O’Brien and H. Farid, “Exposing photo manipulation with inconsistent reflections,” *ACM Transactions on Graphics*, vol. 31, no. 1, p. 4, 2012.
- [15] M. Fontani, T. Bianchi, A. D. Rosa, A. Piva, and M. Barni, “A framework for decision fusion in image forensics based on dempster-shafer theory of evidence,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 593–607, 2013.
- [16] M. K. Johnson and H. Farid, “Exposing digital forgeries by detecting inconsistencies in lighting,” in *ACM Multimedia and Security Workshop*, pp. 1–10, 2005.
- [17] M. K. Johnson and H. Farid, “Exposing digital forgeries through specular highlights on the eye,” in *Information Hiding*, pp. 311–325, 2007.

- [18] M. K. Johnson and H. Farid, “Exposing digital forgeries in complex lighting environments,” *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3-1, pp. 450–461, 2007.
- [19] W. Zhang, X. Cao, J. Zhang, J. Zhu, and P. Wang, “Detecting photographic composites using shadows,” in *IEEE International Conference on Multimedia and Expo*, pp. 1042–1045, 2009.
- [20] P. Kakar and N. Sudha, “Verifying temporal data in geotagged images via sun azimuth estimation,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1029–1039, 2012.
- [21] E. Kee, J. F. O’Brien, and H. Farid, “Exposing photo manipulation with inconsistent shadows,” *ACM Transactions on Graphics*, vol. 32, no. 3, p. 28, 2013.
- [22] V. Conotter, G. Boato, and H. Farid, “Detecting photo manipulation on signs and billboards,” in *Proc. of International Conference on Image Processing*, pp. 1741–1744, 2010.
- [23] E. Kee and H. Farid, “Detecting photographic composites of famous people,” Tech. Rep. TR2009-656, Department of Computer Science, Dartmouth College, 2009.
- [24] S. Zhu, X. Cao, and H. Zhao, “Photographic composite detection using two circles,” in *Sixth International Conference on Image and Graphics*, pp. 858–863, 2011.
- [25] M. K. Johnson and H. Farid, “Exposing digital forgeries through chromatic aberration,” in *Proc. of ACM Multimedia and Security Workshop*, pp. 48–55, 2006.
- [26] I. Yerushalmy and H. Hel-Or, “Digital image forgery detection based on lens and sensor aberration,” *International Journal of Computer Vision*, vol. 92, no. 1, pp. 71–91, 2011.

- [27] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, “Source camera identification using footprints from lens aberration,” in *SPIE Conference on Digital Photography*, vol. 6069, pp. 60690J–60690J–8, 2006.
- [28] J. Lukáš, J. Fridrich, and M. Goljan, “Detecting digital image forgeries using sensor pattern noise,” in *SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents*, vol. 6072, 2006.
- [29] C.-T. Li, “Source camera identification using enhanced sensor pattern noise,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, p-p. 280–287, 2010.
- [30] A. E. Dirik, H. Sencar, and N. Memon, “Source camera identification based on sensor dust characteristics,” in *IEEE Workshop on Signal Processing Applications for Public Security and Forensics*, pp. 1–6, 2007.
- [31] A. E. Dirik, H. T. Sencar, and N. D. Memon, “Flatbed scanner identification based on dust and scratches over scanner platen,” in *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 1385–1388, 2009.
- [32] Z. Lin, R. Wang, X. Tang, and H.-Y. Shum, “Detecting doctored images using camera response normality and consistency,” in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 1, pp. 1087–1092 vol. 1, 2005.
- [33] Y.-F. Hsu and S.-F. Chang, “Camera response functions for image forensics: An automatic algorithm for splicing detection,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 816–825, 2010.
- [34] T.-T. Ng and M.-P. Tsui, “Camera response function signature for digital forensics c- part i: Theory and data selection,” in *IEEE Workshop on Information Forensics and Security*, pp. 156–160, dec 2009.

- [35] T.-T. Ng, “Camera response function signature for digital forensics - part ii: Signature extraction,” in *First IEEE International Workshop on Information Forensics and Security*, pp. 161–165, 2009.
- [36] H. Cao and A. C. Kot, “Similar dslr processor identification using compact model templates,” in *Asia Pacific Signal and Information Processing Association*, 2011.
- [37] S. Ye, Q. Sun, and E.-C. Chang, “Detecting digital image forgeries by measuring inconsistencies of blocking artifact,” in *IEEE International Conference on Multimedia and Expo*, pp. 12–15, 2007.
- [38] Z. Qu, W. Luo, and J. Huang, “Identifying shifted double jpeg compression artifacts for non-intrusive digital image forensics,” in *First International Conference on Computational Visual Media*, pp. 1–8, 2012.
- [39] T.-T. Ng, S.-F. Chang, and Q. Sun, “Blind detection of photomontage using higher order statistics,” in *Proc. of International Symposium on Circuits and Systems*, pp. 688–691, 2004.
- [40] M. C. Stamm and K. J. R. Liu, “Forensic detection of image manipulation using statistical intrinsic fingerprints,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 492–506, 2010.
- [41] E. Kee, M. K. Johnson, and H. Farid, “Digital image authentication from jpeg headers,” *IEEE Transactions on Information Forensics and Security*, 2011.
- [42] A. C. Popescu and H. Farid, “Exposing digital forgeries in color filter array interpolated images,” *IEEE Transactions on Signal Processing*, vol. 53, pp. 3948–3959, 2005.
- [43] A. Swaminathan, M. Wu, and K. J. R. Liu, “Digital image forensics via intrinsic fingerprints,” *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 101–117, 2008.

- [44] J. He, Z. Lin, L. Wang, and X. Tang, “Detecting doctored jpeg images via dct coefficient analysis,” in *European Conference on Computer Vision*, pp. 423–435, 2006.
- [45] M. Chen, J. Fridrich, M. Goljan, and J. Lukás, “Determining image origin and integrity using sensor noise,” *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, 2008.
- [46] H. Farid, “Exposing digital forgeries from jpeg ghosts,” *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 1, pp. 154–160, 2009.
- [47] H. Farid, “Photo fakery and forensics,” *Advances in Computers*, vol. 77, pp. 1–55, 2009.
- [48] A. E. Dirik and N. D. Memon, “Image tamper detection based on demosaicing artifacts,” in *Proc. of International Conference on Image Processing*, pp. 1497–1500, 2009.
- [49] P. Sutthiwan, Y.-Q. Shi, J. Dong, T. Tan, and T.-T. Ng, “New developments in color image tampering detection,” in *International Symposium on Circuits and Systems*, pp. 3064–3067, 2010.
- [50] H. Farid and M. J. Bravo, “Image forensic analyses that elude the human visual system,” in *Media Forensics and Security*, p. 754106, 2010.
- [51] J. Fridrich, D. Soukal, and J. Lukas, “Detection of copy move forgery in digital images,” in *Digital Forensic Research Workshop*, aug 2003.
- [52] T.-T. Ng and S.-F. Chang, “A model for image splicing,” in *Proc. of International Conference on Image Processing*, pp. 1169–1172, 2004.
- [53] W. Luo, J. Huang, and G. Qiu, “Robust detection of region-duplication forgery in digital image,” in *18th International Conference on Pattern Recognition*, vol. 4, pp. 746–749, 2006.

- [54] Y.-F. Hsu and S.-F. Chang, “Detecting image splicing using geometry invariants and camera characteristics consistency,” in *International Conference on Multimedia and Expo*, 2006.
- [55] Y.-F. Hsu and S.-F. Chang, “Image splicing detection using camera response function consistency and automatic segmentation,” in *International Conference on Multimedia and Expo*, 2007.
- [56] M. K. Johnson and H. Farid, “Detecting photographic composites of people,” in *Proc. of the 6th International Workshop on Digital Watermarking*, Lecture Notes in Computer Science, (Berlin, Heidelberg), pp. 19–33, Springer, 2008.
- [57] W. Zhang, X. Cao, Z. Feng, J. Zhang, and P. Wang, “Detecting photographic composites using two-view geometrical constraints,” in *IEEE International Conference on Multimedia and Expo*, pp. 1078–1081, 2009.
- [58] Q. Zheng, W. Sun, and W. Lu, “Digital spliced image forensics based on edge blur measurement,” in *IEEE International Conference on Information Theory and Information Security*, pp. 399–402, 2010.
- [59] W. Zhang, X. Cao, Y. Qu, Y. Hou, H. Zhao, and C. Zhang, “Detecting and extracting the photo composites using planar homography and graph cut,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 544–555, 2010.
- [60] B. L. Shivakumar and S. S. Baboo, “Detecting copy-move forgery in digital images: A survey and analysis of current methods,” *Global Journal of Computer Science and Technology*, vol. 10, no. 7, pp. 61–65, 2011.
- [61] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, “A SIFT-based forensic method for copy-move attack detection and transformation recovery,” *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 1099–1110, Sep. 2011.

- [62] Q. Liu, X. Cao, C. Deng, and X. Guo, “Identifying image composites through shadow matte consistency,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3-2, pp. 1111–1122, 2011.
- [63] D. Vazquez-Padin and F. Pérez-González, “Exposing original and duplicated regions using sift features and resampling traces,” in *International Workshop on Digital Watermarking*, pp. 306–320, 2011.
- [64] S. Zhu, X. Cao, and H. Zhao, “Photographic composite detection using circles,” *Frontiers of Computer Science*, vol. 6, no. 6, pp. 741–755, 2012.
- [65] L. Wu, X. Cao, W. Zhang, and Y. Wang, “Detecting image forgeries using metrology,” *Machine Vision and Applications*, vol. 23, no. 2, pp. 363–373, 2012.
- [66] H. Fu and X. Cao, “Forgery authentication in extreme wide-angle lens using distortion cue and fake saliency map,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1301–1314, 2012.
- [67] J. Chen, H. Zhao, Y. Han, and X. Cao, “Visual saliency detection based on photographic composition,” in *Proc. of the Fifth International Conference on Internet Multimedia Computing and Service*, pp. 13–16, 2013.
- [68] G. Lynch, F. Y. Shih, and H.-Y. M. Liao, “An efficient expanding block algorithm for image copy-move forgery detection,” *Information Sciences*, vol. 239, pp. 253–265, 2013.
- [69] S. Bayram, H. T. Sencar, and N. D. Memon, “An efficient and robust method for detecting copy-move forgery,” in *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 1053–1056, 2009.
- [70] P. Kakar, N. Sudha, and W. Ser, “Detecting digital image forgeries through inconsistent motion blur,” in *IEEE International Conference on Multimedia and Expo*, pp. 486–491, 2010.

- [71] M. Barni, A. Costanzo, and L. Sabatini, "Identification of cut & paste tampering by means of double-jpeg detection and image segmentation," in *Proc. of IEEE International Symposium on Circuits and Systems*, pp. 1687–1690, 2010.
- [72] P. Kakar, N. Sudha, and W. Ser, "Exposing digital image forgeries by detecting discrepancies in motion blur," *IEEE Transactions on Multimedia*, vol. 13, no. 3, pp. 443–452, 2011.
- [73] P. Kakar and N. Sudha, "Exposing postprocessed copy-paste forgeries through transform-invariant features," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1018–1028, 2012.
- [74] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Transactions on Signal Processing*, vol. 53, no. 2-2, pp. 758–767, 2005.
- [75] B. Mahdian and S. Saic, "Detection of resampling supplemented with noise inconsistencies analysis for image forensics," in *International Conference on Computational Sciences and Its Applications*, pp. 546–556, 2008.
- [76] W. Luo, J. Huang, and G. Qiu, "Jpeg error analysis and its applications to digital image forensics," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 480–491, 2010.
- [77] G. Cao, Y. Zhao, and R. Ni, "Forensic estimation of gamma correction in digital images," in *Proc. of International Conference on Image Processing*, pp. 2097–2100, 2010.
- [78] H. Farid, "Blind inverse gamma correction," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1428–1433, 2001.
- [79] J. Lukáš and J. Fridrich, "Estimation of primary quantization matrix in double compressed jpeg images," in *Proc. of Digital Forensic Research Workshop*, Aug 2003.

- [80] A. Swaminathan, M. Wu, and K. J. R. Liu, "A component estimation framework for information forensics," in *IEEE 9th Workshop on Multimedia Signal Processing*, pp. 397–400, 2007.
- [81] W. Wei, S. Wang, and Z. Tang, "Estimation of rescaling factor and detection of image splicing," in *11th IEEE International Conference on Communication Technology*, pp. 676–679, 2008.
- [82] W. Wei, S. Wang, X. Zhang, and Z. Tang, "Estimation of image rotation angle using interpolation-related spectral signatures with application to blind detection of image forgery," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 507–517, 2010.
- [83] H. Su, W.-H. Chuang, W. Lu, and M. Wu, "Evaluating the quality of individual sift features," in *Proc. of International Conference on Image Processing*, pp. 2377–2380, 2012.
- [84] J. Lukas, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, 2006.
- [85] A. Swaminathan, M. Wu, and K. J. R. Liu, "Nonintrusive component forensics of visual sensors using output images," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 91–106, 2007.
- [86] H. Gou, A. Swaminathan, and M. Wu, "Noise features for image tampering detection and steganalysis," in *Proc. of International Conference on Image Processing*, pp. 97–100, 2007.
- [87] A. E. Dirik, H. T. Sencar, and N. D. Memon, "Digital single lens reflex camera identification from traces of sensor dust," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 539–552, 2008.

- [88] A. C. Gallagher and T. Chen, “Image authentication by detecting traces of demosaicing,” *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, vol. 0, pp. 1–8, 2008.
- [89] C. McKay, A. Swaminathan, H. Gou, and M. Wu, “Image acquisition forensics: Forensic analysis to identify imaging source,” in *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 1657–1660, 2008.
- [90] E. Kee and H. Farid, “Printer profiling for forensics and ballistics,” in *Proc. of the 10th ACM workshop on Multimedia and security*, pp. 3–10, 2008.
- [91] G. Bloy, “Blind camera fingerprinting and image clustering,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 30, no. 3, pp. 532–534, 2008.
- [92] Y. Fang, A. E. Dirik, X. Sun, and N. D. Memon, “Source class identification for dslr and compact cameras,” in *IEEE International Workshop on Multimedia Signal Processing*, pp. 1–5, 2009.
- [93] H. Cao and A. C. Kot, “Accurate detection of demosaicing regularity for digital image forensics,” *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 899–910, 2009.
- [94] M. Barni and B. Tondi, “The source identification game: An information-theoretic perspective,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 450–463, 2013.
- [95] H. Cao and A. C. Kot, “Detection of tampering inconsistencies on mobile photos,” in *Digital Watermarking*, vol. 6526 of *Lecture Notes in Computer Science*, pp. 105–119, 2011.
- [96] H. Cao and A. C. Kot, “Mobile camera identification using demosaicing features,” in *Proc. of IEEE International Symposium on Circuits and Systems*, pp. 1683–1686, 2010.

- [97] H. Gou, A. Swaminathan, and M. Wu, “Intrinsic sensor noise features for forensic analysis on scanners and scanned images,” *IEEE Transactions on Information Forensics and Security*, vol. 4, pp. 476–491, 2009.
- [98] H. Yu, T.-T. Ng, and Q. Sun, “Recaptured photo detection using specular-ity distribution,” in *Proc. of International Conference on Image Processing*, pp. 3140–3143, 2008.
- [99] H. Cao and A. C. Kot, “Identification of recaptured photographs on lcd screens,” in *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 1790–1793, 2010.
- [100] S. Lyu and H. Farid, “How realistic is photorealistic?,” *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 845–850, 2005.
- [101] T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M.-P. Tsui, “Physics-motivated features for distinguishing photographic images and computer graphics,” in *ACM Multimedia*, pp. 239–248, 2005.
- [102] Y. Wang and P. Moulin, “On discrimination between photorealistic and photographic images,” in *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 2, pp. 161–164, 2006.
- [103] Y. Chen, Z. Li, M. Li, and W.-Y. Ma, “Automatic classification of photographs and graphics,” in *IEEE International Conference on Multimedia and Expo*, pp. 973–976, 2006.
- [104] H. Farid and M. J. Bravo, “Perceptual discrimination of computer generated and photographic faces,” *Digital Investigation*, vol. 8, no. 3-4, pp. 226–235, 2012.
- [105] R. Zhang, R.-D. Wang, and T.-T. Ng, “Distinguishing photographic images and photorealistic computer graphics using visual vocabulary on local image edges,” in *Lecture Notes in Computer Science Digital Forensics and Watermarking*, pp. 292–305, 2011.

- [106] J. Mao, O. Bulan, G. Sharma, and S. Datta, “Device temporal forensics: An information theoretic approach,” in *Proc. of International Conference on Image Processing*, pp. 1501–1504, 2009.
- [107] A. D. Rosa, F. Uccheddu, A. Costanzo, A. Piva, and M. Barni, “Exploring image dependencies: a new challenge in image forensics,” in *Proc. SPIE 7541, Media Forensics and Security II*, 2010.
- [108] J. Fridrich and M. Goljan, “Determining approximate age of digital images using sensor defects,” in *Proc. SPIE Media Watermarking, Security, and Forensics III*, vol. 7880, pp. 06–11, 2011.
- [109] A. L. Varna and M. Wu, “Modeling temporal correlations in content fingerprints,” in *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1860–1863, 2011.
- [110] I. Avcibas, N. Memon, and B. Sankur, “Steganalysis using image quality metrics,” *IEEE Transactions on Image Processing*, vol. 12, pp. 221–229, 2003.
- [111] I. Avcibas, M. Kharrazi, N. D. Memon, and B. Sankur, “Image steganalysis with binary similarity measures,” *Journal of applied singal precessing*, vol. 2005, no. 17, pp. 2749–2757, 2005.
- [112] S. Lyu and H. Farid, “Steganalysis using higher-order image statistics,” *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 1, pp. 111–119, 2006.
- [113] T. Pevny and J. Fridrich, “Detection of double-compression in jpeg images for applications in steganography,” *IEEE Transactions on Information Forensics and Security*, vol. 3, pp. 247–258, June 2008.
- [114] G. Valenzise, V. Nobile, M. Tagliasacchi, and S. Tubaro, “Countering jpeg anti-forensics,” in *Proc. of the 18th IEEE International Conference on Image Processing*, pp. 1949–1952, 2011.

- [115] H. Li, W. Luo, and J. Huang, “Countering anti-jpeg compression forensics,” in *Proc. of International Conference on Image Processing*, pp. 241–244, 2012.
- [116] W.-H. Chuang and M. Wu, “Robustness of color interpolation identification against anti-forensic operations,” in *Information Hiding*, pp. 16–30, 2012.
- [117] I. Amerini, M. Barni, R. Caldelli, and A. Costanzo, “Counter-forensics of sift-based copy-move detection by means of keypoint classification,” *EURASIP Journal Image and Video Processing*, vol. 2013, p. 18, 2013.
- [118] H. T. Sencar and N. Memon, *Overview of State-of-the-art in Digital Image Forensics, Part of Indian Statistical Institute Platinum Jubilee Monograph series titled “Statistical Science and Interdisciplinary Research”*. World Scientific Press, 2008.
- [119] T. V. Lanh, K.-S. Chong, S. Emmanuel, and M. S. Kankanhalli, “A survey on digital camera image forensic methods,” in *IEEE International Conference on Multimedia and Expo*, pp. 16–19, 2007.
- [120] W. Luo, Z. Qu, F. Pan, and J. Huang, “A survey of passive technology for digital image forensics,” *Frontiers of Computer Science in China*, vol. 1, no. 2, pp. 166–179, 2007.
- [121] H. Farid, “A survey of image forgery detection,” *IEEE Signal Processing Magazine*, vol. 2, no. 26, pp. 16–25, 2009.
- [122] J. Fridrich, “Image watermarking for tamper detection,” in *Proc. of International Conference on Image Processing*, vol. 2, pp. 404–408, 1998.
- [123] A. D’Angelo, G. Cancelli, and M. Barni, “Watermark-based authentication,” in *Intelligent Multimedia Analysis for Security Applications*, pp. 365–402, 2010.
- [124] M. Schäler, S. Schulze, R. Merkel, G. Saake, and J. Dittmann, “Reliable provenance information for multimedia data using invertible fragile watermarks,” in *Advances in Databases, Lecture Notes in Computer Science*, pp. 3–17, 2011.

- [125] G. Friedman, “The trustworthy digital camera: restoring credibility to the photographic image,” *IEEE Transactions on Consumer Electronics*, vol. 39, no. 4, pp. 905–910, 1993.
- [126] JEIDA, “Design rule for camera file system version 1.0.” <http://www.exif.org/dcf.PDF>, October 1995.
- [127] JEIDA, “Design rule for camera file system version 2.0.” <http://ceres.informatik.fh-kl.de/pbw/lehre/20041/foto/ressourcen/Dokumentation/Exif/cp3461.pdf>, July 1998.
- [128] JEIDA, “Design rule for camera file system version 2.1.” <http://www.exif.org/dcf.PDF>, January 1999.
- [129] JEIDA, “Overview of the revisions to the dcf and exif standards.” http://www.cipa.jp/exifprint/contents_e/01exif_e/ExifDCFsummary_E.pdf, July 2003.
- [130] A. D. Association, “Tiff revision 6.0, month = June, year = 1992, howpublished = ”<http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf>”.”
- [131] G. Bo and J. Ramesh, “Segmenting photo streams in events based on optical metadata,” in *Proc. of the International Conference on Semantic Computing*, (Washington, DC, USA), pp. 71–78, IEEE Computer Society, 2007.
- [132] W. Ku, M. S. Kankanhalli, and J.-H. Lim, “Using camera settings templates (“scene modes”) for image scene classification of photographs taken on manual/expert settings,” in *Proc. of the multimedia 8th Pacific Rim conference on Advances in multimedia information processing*, (Berlin, Heidelberg), pp. 10–17, Springer-Verlag, 2007.
- [133] C.-J. Jang, J.-Y. Lee, J.-W. Lee, and H.-G. Cho, “Smart management system for digital photographs using temporal and spatial features with exif metadata,” in *2nd International Conference on Digital Information Management*, pp. 110–115, 2007.

- [134] B. Matthew and L. Jiebo, “Photo classification by integrating image content and camera metadata,” in *Proc. of the 17th International Conference on Pattern Recognition*, vol. 4, (Washington, DC, USA), pp. 901–904, IEEE Computer Society, 2004.
- [135] J. Yuan, J. Luo, H. S. Kautz, and Y. Wu, “Mining gps traces and visual words for event classification,” in *Multimedia Information Retrieval*, pp. 2–9, 2008.
- [136] X. Sun, J. Sun, J. Zhang, and M. Li, “Simple zoom-lens digital camera calibration method based on exif,” vol. 5302, pp. 79–86, *Proc. SPIE 5302, Three-Dimensional Image Capture and Applications VI*, 2004.
- [137] H.-C. Huang, W.-C. Fang, and S.-C. Chen, “Copyright protection with exif metadata and error control codes,” in *Proc. of the 2008 International Conference on Security Technology*, (Washington, DC, USA), pp. 133–136, IEEE Computer Society, 2008.
- [138] H.-C. Huang, W.-C. Fang, and S.-C. Chen, “Privacy protection and authentication for medical images with record-based watermarking,” in *Life Science Systems and Applications Workshop*, pp. 190 –193, 9-10 2009.
- [139] R. Ramanath, W. Snyder, Y. Yoo, and M. Drew, “Color image processing pipeline,” *IEEE Signal Processing Magazine*, vol. 22, no. 1, pp. 34–43, 2005.
- [140] Z. Deng, A. Gijsenij, and J. Zhang, “Source camera identification using auto-white balance approximation,” in *IEEE International Conference on Computer Vision*, pp. 57–64, 2011.
- [141] J. R. Janesick, *Scientific Charge-Coupled Devices*. Bellingham, WA: SPIE Press, 2001.
- [142] G. C. Holst and T. S. Lomheim, *CMOS/CCD sensors and camera systems*. Society of Photo Optical, 2007.

- [143] D. Wueller and R. Fageth, “Statistic analysis of millions of digital photos,” vol. 6817, p. 68170L, SPIE, 2008.
- [144] J. Wiley and Sons, *A Technical Introduction to Digital Video*. New York: John Wiley and Sons, 1996.
- [145] R. E. Jacobson, *The manual of photography : a textbook of photographic and digital imaging*. Oxford : Focal, 9th ed., 2000. Previous ed.: 1988.
- [146] P. Pudil, F. Ferri, J. Novovicova, and J. Kittler, “Floating search methods for feature selection with nonmonotonic criterion functions,” in *Proc. of International Conference on Pattern Recognition*, vol. 2, pp. 279–283, 1994.
- [147] I. Avcibas, S. Bayram, N. D. Memon, M. Ramkumar, and B. Sankur, “A classifier design for detecting image manipulations,” in *Proc. of International Conference on Image Processing*, pp. 2645–2648, 2004.
- [148] G. D. Finlayson, M. S. Drew, and B. V. Funt, “Diagonal transforms suffice for color constancy,” in *IEEE International Conference on Computer Vision*, pp. 164–171, 1993.
- [149] S. E. Susstrunk, J. M. Holm, and G. D. Finlayson, “Chromatic adaptation performance of different rgb sensors,” in *SPIE Proc. Color Imaging: Device-Independent Color, Color Hardcopy, and Graphic Arts VI*, vol. 4300, (San Jose, CA), pp. 172–183, 2001.
- [150] B. Lindbloom, “Chromatic adaptation,” *Bruce J. Lindbloom, Tech. Rep*, 2007.
- [151] G. Finlayson and E. Trezzi, “Shades of gray and colour constancy,” in *Proc. of the 12th Color Imaging Conference on Society for Imaging Science and Technology*, pp. 37–41, 2004.
- [152] J. van de Weijer, T. Gevers, and A. Gijsenij, “Edge-based color constancy,” *IEEE Transactions on Image Processing*, vol. 16, pp. 2207–2214, 2007.

- [153] A. Eskicioglu and P. Fisher, “Image quality measures and their performance,” *IEEE Transactions on Communications*, vol. 43, no. 12, pp. 2959–2965, 1995.
- [154] T. Frese, C. Bouman, and J. P. Allebach, “Methodology for designing image similarity metrics based on human visual system models,” in *Proc. SPIE Conference on Human Vision and Electronic Imaging II*, vol. 3016, pp. 472–483, 1997.
- [155] X. Jiang, B. Mandal, and A. C. Kot, “Eigenfeature regularization and extraction in face recognition,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 30, pp. 383–394, mar 2008.