Use of defocus blur consistency to detect Image Forgery

Prepared By

Ankit Prajapati

12MCEI39

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

MAY 2014

Use of defocus blur consistency to detect Image Forgery

Major Project

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology in Computer Science and Engineering With Specialization in Information And Network Security

Prepared By

Ankit Prajapati

(12MCEI39)

Guided By

Prof. Pooja Shah

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

MAY 2014

Certificate

This is to certify that the Major Project Report entitled "**Use of defocus blur consistency to detect Image Forgery**" submitted by **Ankit Prajapati(Roll No: 12MCEI39)**, towards the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering with specialization in Information and Network Security of Nirma University, Ahmedabad is the record of work carried out by her under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project part-I, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Prof. Pooja Shah
Guide & Assistant Professor,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Prof. Sharada Valiveti
Associate Professor
Coordinator M.Tech - CSE(INS)
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Sanjay Garg
Professor and Head,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr K Kotecha
Director,
Institute of Technology,
Nirma University, Ahmedabad

Undertaking for Originality of the Work

I, **Ankit Prajapati**, Roll. No. **12MCEI39**, give undertaking that the Major Project entitled "**Use of defocus blur consistency to detect Image Forgery**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science & Engineering with specialization in Information and Network Security** of Nirma University, Ahmedabad, is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

_____

Signature of Student

Date:

Place:

Endorsed by

Prof. Pooja Shah

(Signature of Guide)

Acknowledgements

It gives me immense pleasure in expressing thanks and profound gratitude to **Prof. Pooja P. Shah**, Professor, Computer Science Department, Institute of Technology, Nirma University, Ahmedabad for her valuable guidance and continual encouragement throughout this work. The appreciation and continual support she has imparted has been a great motivation to me in reaching a higher goal. Her guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

My deepest thank you is extended to **Prof. Sharada Valiveti**, PG CSE(INS) - Coordinator, Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad for an exceptional support and continual encouragement throughout the Major Project.

It gives me an immense pleasure to thank **Dr. Sanjay Garg**, Hon'ble Head of Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed wholeheartedly to **Dr K Kotecha**, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation he has extended throughout course of this work.

I would also thank the Institution, all faculty members of Computer Engineering Department, Nirma University, and Ahmedabad for their special attention and suggestions towards the project work.

The blessings of God and family members make the way for completion of Project. I am very much grateful to them.

- Ankit Prajapati

12MCEI39

Abstract

A method of defocus blur consistency to detect image forgery has been introduced in this paper. At each edge pixel is estimated for the local blur this reveals the defocus blur inconsistency. The results that obtained are effective hence have good applications in real world which consists of tampered images. There is one model i.e., defocus model it has a phenomena that blur sizes of the kernel sizes would be similar for the patches that have similar distance and this gives raise to image forgery crimes that takes advantage of dissimilar imaging conditions and possibility of blurring. In case of quality of real and virtual image obtained because of blurring motion and defocusing easily shows the seam between both virtual and real word. So the solution of the problem is video see-through augmented reality, this consists of simulations of the optical system of camera when rendering of the virtual objects takes place.

Key words: Image tampering; Forgery; blur consistancy to detect image forgery.

Contents

List of Figures

Chapter 1

Introduction

Image forgery Is old concept, dating back to 1840s,when hippolyta bayard produced first fake image of him committing suicide, in frustration of losing the chance of becoming of inventor of photography to Louis Dnaguerre.
Advanced Image Forgery does not vary truly in nature contrasted with tried and true Image Forgery. As opposed to utilizing photo, computerized picture imitation arrangements with advanced image. Creating a forged image process is simple with powerful computer graphics modified by some software For example Corel Paint shop, GIMP, Photoshop or some other which are easily available on many websites.

There are numerous instances of advanced picture falsification. These cases could be classified into three real gatherings, in view of the methodology included in making the fake picture. They are 1) Image Retouching.
2) Image Splicing.
Copy-Move Attack.

Image Retouching might be recognized to be the less destructive sort of digital picture imitation. Image retouching does not fundamentally change a picture, however rather, improves or diminishes certain characteristic of a picture. This procedure is prevalent among magazine photograph editors. It might be said that just about all magazine spread might utilize this method to "upgrade" certain characteristics of a picture so it is more alluring; disregarding the way that such improvement is morally off base. Image Splicing is more forceful than image retouching. Image Splicing is a strategy that includes a

composite of two or more pictures which are joined together to make a fake picture.

copy move attack is pretty much like Image Splicing in perspective of the way that both systems change certain image area (of a base picture), with an alternate picture. Nonetheless, as opposed to having an external image as the source, copy move attack utilizes part of the first base picture as its source. At the end of the day, the source and the objective of the adjusted picture began from the same picture. In a copy move attack, parts of the first picture is duplicated, moved to a coveted area, and stuck. This is typically done to cover certain subtle elements or to double certain parts of a picture. Blurring is usually applied along the border of the modified region to lessen the impact of irregularities between the first and stuck region.

Active and Passive approached are two methods for detect to digital image forgery. Active method is a some pre-processing requirement for image for example watermarking or signature that is generate at creating time, it is the limitation of this technique. Also, there are a large number of advanced pictures in web without digital signature or watermark. In such situation dynamic methodology couldn't be utilized to discover the authentication of the picture.

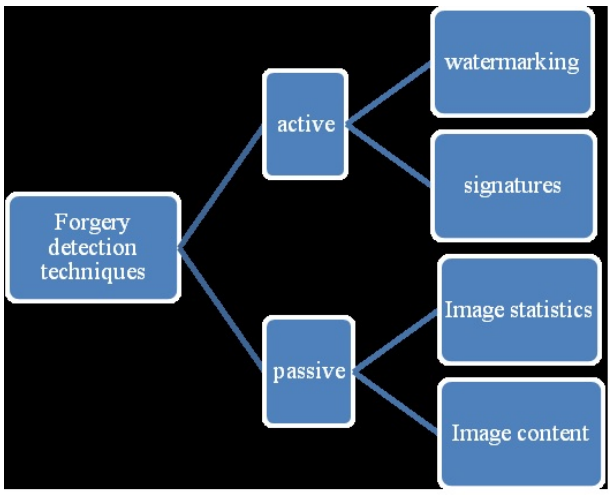

Figure 1.1: Classification of Forgery detection techniquies.

Dissimilar to the watermark-based and signature based routines; the uninvolved innovation does not require any digital signature created or watermark inserted ahead of

time. When the absence of the watermark and signature the passive method used for the image forensics. These methods chip away at the suspicion that albeit digital falsifications may leave no visual intimations that indicate tampering, they may adjust the underlying detail of a picture.

Picture falsification manages changing the observation of the individual who is taking a gander at the picture or you can say spectator. Much programming is accessible today that can give the office of altering the pictures and that might be possible effectively. Picture altering is presently pulling in numerous programmers and distinctive class of individual included in unlawful acts. So discovering answer for that fabrication is equitably an inquisitive assignment. As the force of the product has expanded controlling the advanced pictures is a convenient errand.

Water marking and signature are the basically utilized authentication plan. The fundamental necessity of the these systems is data inserted in the picture. At the same time here is a drawback that for the most part digital imaging gadgets don't embed data in pictures. Subsequently the passive blind image crime scene investigation has no former reference of the modifications that has been made and it is a complex issue with no widespread result.

Image formation methodology when the center is on the object point and light beams emanated from the point and caught by the lens meet at a point on the picture plane when the thin lens of true opening camera is being used. In any case when the object point is not in center, the picture that is shaped is a circular patch; the radius of this characterizes the measure of defocus connected with the depth of the point introduce in the scene. This states that reasonability is available between the depth of the point and defocus blur radius.

The set of image forensic tools can be roughly grouped into five categories:

1 pixel-based procedures that detect stastical anomalies presented at the pixel level: The legitimate framework routinely depends on an extent of forensic analysis examination going from measurable ID (Deoxyribonucleic corrosive (DNA) or finger impression) to criminological odontology (teeth), forensic entomology (creepy crawlies), and forensic geography (soil). In the customary forensic sciences, all way

of physical confirmation is investigated. In the digital area, the accentuation is on the pixelthe underlying building block of an advanced picture. I depict four strategies for distinguishing different manifestations of altering, each of which specifically or in a roundabout way dissects pixel-level relationships that emerge from a particular manifestation of altering. In pixel-based procedure four sort of identification are characterized 1)cloning,2) Re-testing , 3) Splicing , 4) Statistical

2 Format based procedures that influence the factual relationships presented by a particular lossy compression plan: The first govern in any forensic examination should definitely be "protect the proof." In this respect, lossy picture layering plans, for example, JPEG may be viewed as a measurable expert's most noticeably awful adversary. It is unexpected, accordingly, that the extraordinary properties of lossy packing could be abused for scientific investigation. I portray three legal systems that distinguish altering in layered pictures, each of which unequivocally influences points of interest of the JPEG lossy pressure plan. These system characterized three ways 1) JPEG Quantization , 2) Double JPEG and 3) JPEG blocking.

3 Camera based method exploit artifacts which is described by sensor onchip post-processing and camera lens. In the same spirit, several image forensic techniques have been developed that specifically model artifacts introduced by various stages of the imaging process. Chromatic Aberration,color Filter array,Camera response and Sensor Noise are the method to detect fake image to calculate different camera artifacts and modeling.

4 Physically based: Physically based procedures that expressly demonstrate and catch oddities in the three dimensional association between camera, physical object and light. Suppose creating fake image to show two stars of movie, reputed to be impractically included, strolling down a sunset beach. Many of images may be creating by splicing together separated images of each movie star. Some time difficult to match exactly in lighting effect under each people was actual photograph. Describe for calculate different properties of lighting environment under which part of people or object was photographed of three method. 1) Contrasts in lighting over a picture can then be utilized as confirmation of altering. 2) Direction of light (2-D and 3-D) and 3) Environment of light.

5 Geometric-based: These techniques make measurements of particular objects in real world and their positions with respect to the Polaroid [1]: Two principle is used for detect image forgery in these technique 1) Projection of the camera center onto the image plane 2)The metric measurements

Chapter 2

Motivation For Development

Recently many researchers is increasing the photometric consistency [2,3,4]. The main focus on the shadow and shading of the virtual objects along with some attempts on the quality of virtual objects in the image .Considering the video see-through augmented reality, the seamlessness of the real and virtual worlds is affected by the differences in image quality between superimposed virtual objects and the real image affects and main cause of the problem is the difference of the real and virtual camera models. An ideal camera model is one in which the lens does not degrade the image quality while when rendering virtual objects. As far as a real camera is concerned, the image it captures shows deterioration. Certain attempts have been done to bring down the distinction between real and virtual worlds, like changing the image quality, through which we can change real image and produce virtual objects image quality with cartoon-like or sketch like representation [5,6].

Tampered images have become pervasive:

1. Counterfeiting.
2. Evidence tampering.
3. Antique Faking.
4. Political Propaganda.
5. Scientific Research
6. Entertainment.
7. Urban myths.

Evaluating image deterioration and representing blur effect on virtual objects decides the inconsistency in the real and virtual camera model. Image rehabilitation methods based on evaluating the image degradation, in image processing and computer vision depicted by the point spread function (PSF) has been presented [5]. Calculation wise, involvement of iteration in computing makes these techniques expensive. That is why this kind of technique is not recommended for augmented reality requiring real time operation[7,8].

Despite such advancement, this technique is difficult to apply to augmented reality, the reason being lens parameters. Lens operations always cause the changes; hence needed to be always known and the connected work should calibrate the intrinsic camera parameters. In order to recognize the consistency of image quality in the augmented reality, the main causes of image deterioration- defocusing and motion blurring,, have been covered in this paper. The technique proposed compensates with the real image quality recorded by the real camera along with the virtual objects rendered. Merging of captured image and virtual object rendering with blur effects evaluated from a real scene image containing a marker has been proposed in this method. Along with proposal of a new modified geometric registration methodology which detects the image marker approximately by using the estimated blur parameters and excluding the blur effect from the image captured.

Chapter 3

Literature Survey

1 "Exposing Digital Image Forgeries by Illumination Color Classification"

- Authors::Tiago Jos de Carvalho, Christian Riess,Elli Angelopoulou, Hlio Pedrini and Anderson de Rezende Rocha.
- Journal name and year::IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 7, JULY 2013
- Summary
  * In this paper, One method is discussed that detects counterfeit images of humans using the illuminant color. Make the estimate that an illuminant color being used with a statistical gray edge method and a physics-based method which abuses the inverse intensity-chromaticity color space. It treats like that these illuminant maps and texture maps are equivalent. Second, on these available maps, tear out information on the distribution of edges. We propose new algorithm in order to describe the edge information which is based on edge-points and the HOG descriptor, called HOG edge.
  * The proposed method consists of five main components: 1)Classification. 2)Computation of Illuminant Features. 3)Paired Face Features. 4)Face Extraction. 5)Dense Local Illuminant Estimation (IE).

2 "Pixel Based Digital Image Forgery Detection Techniques"

- Authors::Pradyumna Deshpande , Prashasti Kanikar.

– Journal name and year::International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3 MAY-JUNE 2012.

– Summary

  * We discuss various type of forgery detection techniques. In active approach, some pre-processing tasks such as signature generation or watermark embedding are required by digital images. Due to this, their application is not much practiced. Plus, this approach is not able to find the authentication of the image. Meanwhile, there is no need to be watermark embedded or any digital signature generated in case of the passive technology in advance. In the absence of any watermark or signature, passive techniques operate for image forensics. The assumption has been taken in passive technique that even if they alter the underlying statistics of an image, digital forgeries may leave no visual clues that indicates evidence of tamper.

  * Copy move forgery and algorithms:It is fundamentally picture control sort in which some a piece of the picture itself is repeated and glued into some an alternate a piece of the same picture. This technique is planned to make an article "vanished" from existing picture by blanket it with little piece replicated from an alternate a piece of the same picture. The color palette, noise segments, element range and alternate properties will be good with whatever is left of the picture, since the duplicated portions hail from the same picture. along these lines, to be perceivable by human eye is extremely troublesome. Even here and there, technology may neglect to detect the fake image forgery, if the picture is modified with the accessible apparatuses. In this methodology, as a first venture, with a specific end goal to yield a lessened measurement representation, i.e., Ll1 sub band, DWT is connected to the information picture. As second step, sub-pictures are gotten by Ll1 sub band division. To find the spatial offset (δx, δy) between the Copy-Move districts, stage relationship is embraced. Through pixel-matching, i.e., moving the data picture as indicated by the counterbalance and figuring the contrast between the picture and its

moved form, the Copy-Move areas might be effectively spotted. Finally, to enhance the area, MMO (Mathematical Morphological Operations) are utilized to evacuate segregated focuses..

* Fast Copy- Move Forgery Detection:In fast copy move forgery detection the first block B(16*16) is divides into 4 equal size blocks then calculated average intensity function ave(.). Also ratios of avg entities (f2 to f5) of the blocks s1,s2,s3 and s4 to f1 are calculated. Difference of avg intensities (f6 to f9) are calculated. fi's are normalized to integers xi's (0-255) and radix sort algorithms is used to perform lexicographical sort and shift vectors are defined as the difference of two adjacent vectors. Then finally accumulative number of shift vectors is used to detect duplications.

3 "Image Forgery Detection."

- Authors::Hany Farid..
- Journal name and year::IEEE SIGNAL PROCESSING MAGAZINE. MARCH,2009
- Summary
  * pixel-based procedures that detect stastical anomalies presented at the pixel level: The legitimate framework routinely depends on an extent of forensic analysis examination going from measurable ID (Deoxyribonucleic corrosive (DNA) or finger impression) to criminological odontology (teeth), forensic entomology (creepy crawlies), and forensic geography (soil). In the customary forensic sciences, all way of physical confirmation is investigated. In the digital area, the accentuation is on the pixelthe underlying building block of an advanced picture. I depict four strategies for distinguishing different manifestations of altering, each of which specifically or in a roundabout way dissects pixel-level relationships that emerge from a particular manifestation of altering. In pixel-based procedure four sort of identification are characterized 1)cloning,2) Re-testing , 3) Splicing , 4) Statistical
  * Format based procedures that influence the factual relationships presented by a particular lossy compression plan: The first govern in any forensic examination should definitely be "protect the proof." In this respect, lossy

picture layering plans, for example, JPEG may be viewed as a measurable expert's most noticeably awful adversary. It is unexpected, accordingly, that the extraordinary properties of lossy packing could be abused for scientific investigation. I portray three legal systems that distinguish altering in layered pictures, each of which unequivocally influences points of interest of the JPEG lossy pressure plan. These system characterized three ways 1) JPEG Quantization , 2) Double JPEG and 3) JPEG blocking.

4 "Detecting Logo-Removal Forgery by Inconsistencies of Blur."

- Authors::Jing Zhang, Yuting Su.
- Journal name and year::International Conference on Industrial Mechatronics and Automation,2009
- Summary
  - Another methodology for identifying feature logo-removal forgery is proposed by measuring inconsistencies of blur. In these methodology is focused around the supposition that if an advanced feature experiences logo-removal forgery; the blurriness quality of the fashioned area is relied upon to be distinctive as contrasted with the non-altered parts of the feature. Blurriness is evaluated by the normality properties in the wavelet domain which includes measuring the rot of wavelet change coefficients crosswise over scales. The conveyance of blurriness esteem in a forged video is displayed as a GMM (Gauss Mixture Model). The EM (Expectation-Maximization) calculation is utilized to gauge the model parameters. Therefore, a Bayesian classifier is utilized to discover the ideal edge esteem. Exploratory results indicate that our methodology attains guaranteeing exactness in logo removal forgery detection.
  - To start with, each one frame is apportioned into non covering blocks. The blur of each one piece is assessed by measuring the sharpness of the edges in the square. At that point a straightforward thresholding plan is abused to acquire a coarse grouping. Based on the coarse order, a Gauss Mixture Model is connected to portray the factual circulations of piece blurriness values. The GMM parameters are assessed utilizing

Expectation-Maximization calculation, and the ideal edge is inferred likewise utilizing Bayesian classifier. At long last, since logo's position is static with time, the final blurriness of a given square is dead set as the mean quality of the relating piece values in all frames.

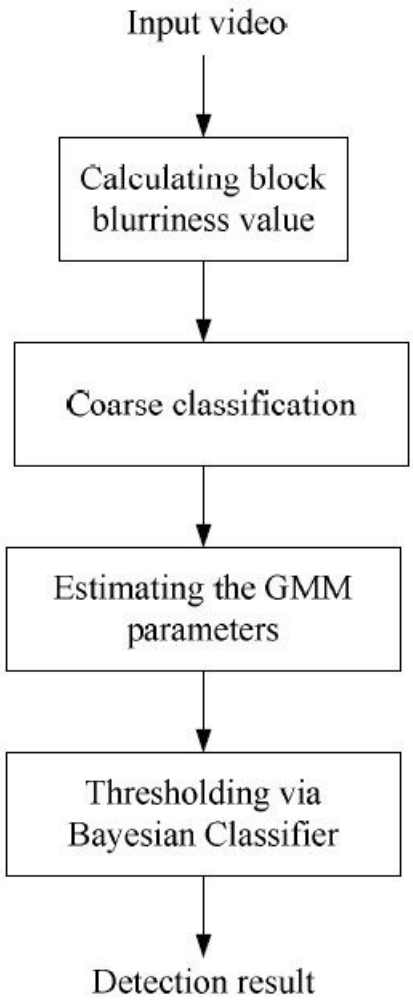

Figure 3.1: Bock Diagram of logo remove model

5 "Digital image forgery detection based on the consistency of defocus blur."

- Authors::Xin Wang, China National Digital Switching System and Bo Xuan, Si-long Peng, National ASIC Design and Engineering Center.
- Journal name and year::International Conference on Intelligent Information Hiding and Multimedia Signal Processing,IEEE,2008

– Summary

* Basic model of defocus:: Picture quality corruption is essentially brought on by noise, shade and blur associating ancient rarities. In a diffraction-constrained lens framework, for example, common digital cameras, diffraction is the fundamental driver of defocus blur. At the point when an object point is not in center, its picture on the picture plane is not a point however a roundabout patch of radius σ that characterizes the measure of defocus connected with the depth of the point in the scene.The radious might be characterized as

$$\sigma = krs\left(\frac{1}{u} + \frac{1}{s} - \frac{1}{f}\right)$$

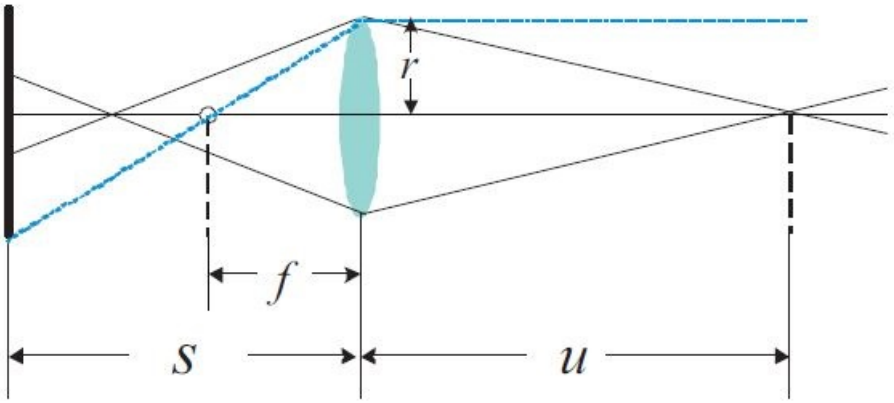

Figure 3.2: A thin lens System

where
r = radius of the aperture
s = distance from lens from image plane
f =focal length
u = depth at that point
= constant that depends on calibration of the camera system.
The thin lens system is shown in Figure.PSF of the camera system at a point (x, y) can be modeled as a circularly symmetric 2-D Gaussian function [Note: PSF = point spread function]

$$h\left(x, y, \sigma_b\right) = \frac{1}{2\pi\sigma_b^2} \mathrm{e}^{-\frac{\left(x^2+y^2\right)}{2\sigma_b^2}}$$

    * Forgery detection method and detection of blur detection

6 "Detecting Digital Tampering by Blur Estimation."

- Authors::Dun-Yu Hsiao, Soo-Chang Pei.
- Journal name and year::IEEE,2005
- Summary
    * Block diagram for digital image forgery creation, face replacement.

7 "Illuminant Color Based Image Forensics."

- Authors::Sandeep Gholap and P. K. Bora.
- Summary
    * Find the forgery in digital images by exploiting colour mismatches among the objects in the image.
    * Forgery detection using illuminant color: The illuminant color is available constantly all around the picture. One weakness while in making composite picture is that there are a few reasons to be different confounds be happened. Two paramount reasons are: 1)the segments of picture which are consolidated together may be under diverse illuminant shades. 2)sometimes, a forgery may change the color of an article to misdirect the evidence.The change in colour will make confuse in the assessment of the illuminant color as for different objects in the picture.

8 "Digital Watermarking Using MATLAB."

- Authors::Pooya Monshizadeh Naini.
- Summary
    * Basic image processing commands in MATLAB.
    * Watermarking Methods.

Chapter 4

Proposed Model

To obtain the blur difference in the real images select a threshold, take real photos clicked from digital cameras of various models with similar u and determine the blur amount of patches. Use 6 real photos having different quality factors. Use content as an image including two persons walking side by side, and some objects like cars,trees, in focus. Blur difference is between 0.08 to 0.2. And two patches blur amount difference with the same distance is more big than T. For more viable angle pick two altered pictures from a true. We should take the picture made by offenders for a monetary cheating. The altered advanced pictures are digitally photoshopped, modified and get filtered. A piece of these pictures are wiped off to secure criminal's protection.

There are three step in this technique:

- First choose patches from images with smooth linear edges also find with similar depth of point(u).
- Now estimates blurriness of both patches image. Also estimates blur edge pixel are calculated as the patch blur.
- Then blurriness clearly different then images is tempered. Also using predefined threshold tell blurriness different and its inconsistency of patch blurs the forgery evidence.

Fig. 4.1 one of the tempered image and detect result on the two people sat on the sofa and patches two images from the tempered image which is shoulder part have same distance to camera lens and differences in such parts. It is found that the blur of patches of Fig. 4.1(b) is 3.2 and much higher than Fig. 4.1(c), 1.7. Also some pixels of blur at

edge pixels is high on fig 5.1(c). when choose edge pixels at the linear smooth in Fig 4.1(c) the difference is clear, which choice of patch is important.

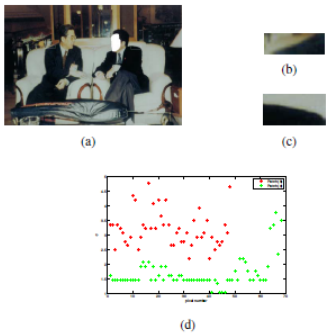

Figure 4.1: (a)Forged image. Two patches chosen for graph. (b)Left patch. (c) Right patch.(d) patches blur amount on egde.

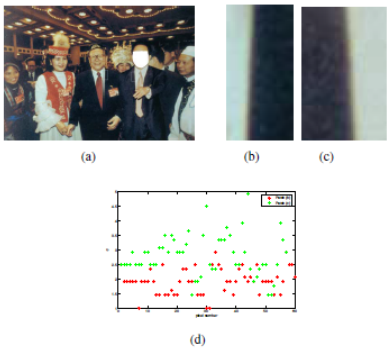

Figure 4.2: (a)Forged image. Two patches chosen for graph. (b)Left patch. (c) Right patch.(d) patches blur amount on egde.

Another forged image in fig 4.2 which show the blur difference 2.8 is small at 1.93 amount.

Chapter 5

Current Work

Some techniques are proposed for render virtual objects with blur effects are in computer graphics:

- Estimations of blur from images:
  In computer field, to restore the distorted image, many methods calculate PSF to models the degradation of image and get back the original image by erasing the PSF effect. These method classified in two approach. One finds the blur effect by analyzing patterns on a target object based on knowledge. Second one has no knowledge about the target objects. An older approach is calculate of the PSF of a scanner [9].Calculate the scanner property which is PSF scanning called patterns and earlier its called blind deconvolution which is recover target objects and it is a set of blurred images. Many techniques are treat the same problem. Depth from defocusing [10, 11,12] and super-resolution [13,14,15] techniques can also be used to estimate the PSF simultaneously.

- Blur representation on virtual objects:
  Several approaches are there to reproduce effects by camera and various techniques render virtual object for realist. For example, Kolb et al.[16] have proposed a rendering strategy recreating an optical arrangement of genuine camera. This system can repeat the focus of center impact which is described by the outline of lens.

5.1 Analysis And Comparision

- 1. Forgery detection method:

  A digital photo is true implies that it is the projection of a genuine 3D scene caught by a digital camera. Accordingly, all parameters with the exception of u in mathematical statement are same for all pixels. Above Equation uncovers that picture point with comparable u ought to have comparative delta however their relationship is not straight in a true photograph. In picture tempering, blurring is frequently connected to the borders of altered areas for better amalgamation. Plus, the imaging states of altered regions and the bacckground picture are diverse with extraordinary probability. These components present the conflict between u and delta and the conflict of defocus blur can go about as the evidence of forgery. Our method pick two picture patches with comparative u and assessment their blurriness. On the off chance that their blurriness is unmistakably diverse, then we judge the picture is altered.

$$\sigma = krs\left(\frac{1}{u} + \frac{1}{s} - \frac{1}{f}\right)$$

  Two patch images in one image is done with similar u and there blurriness is estimated. Patches of blurring are different so it is tampered. If the difference is clear using a predefined threshold. Taking images in regions with some frequency contents then blur can be effectively estimated. Human can easily choose patches image on particular tempered image and estimated blur for every patches image. The conflict of patch blur is the falsification confirmation. We stay away from patches, for example, folded material and shading question and attempt to pick patches with smooth direct edges. In budgetary duplicity cases, the criminal make composite photographs with well-known individuals in political and business area.

- 2. Defocus blur detection:

  To be suitable for forgery identification, the blur estimation strategy must fulfill these conditions:1. Being a local estimation method. Our objective is to gauge the blurriness of small picture patches and the calculate method must be local. 2. Being robust to noise. In picture imitation, the fakers frequently add commotion to the

manufactured picture to conceal phony follow. 3. Having the capacity to manage complex scene structures. The scene structures of genuine common pictures are for the most part perplexing and the blur estimation method must contemplate the scene structures

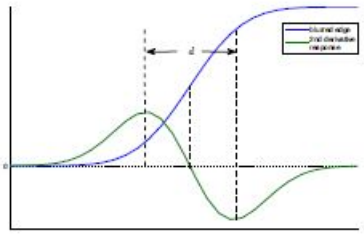

Figure 5.1: Blurred edge and 2nd derivative

Elder and Zucker in[17] are proposed the blur estimation method appropriate. Function $Au\left(x\right)+B$ as a edge in intensity channel. Gaussian blurring kernel $g\left(x,y,\sigma_b\right)=\frac{1}{2\pi\sigma_b^2}\mathrm{e}^{-\frac{\left(x^2+y^2\right)}{2\sigma_b^2}}$ and σ_b is the blur amount. In fig 1, the edge location is the zero crossing in its derivative. The blur amounts to distance between two second derivative extrema with opposite signs. Their method used to calculate scene depth and simulate the shallow depth of field of a lens[17][18]. Elder-Zucker method briefly describe. Firstly, the noise variance of the image need to be calculate. Different from the reference [16], robust estimation $s_n=\frac{median|y_diag|}{0.6745}$, Where $|y_diag|$ is the HH subband with the highest level in wavelet decomposition. Set the significance level for the entire image $\alpha_I=10^{-6}$ and the pixelwise significance level is $\alpha_p=1-\left(1-\alpha_i\right)_n$ where n is the number of pixels.

The gradient is estimated using steerable Gaussian first derivative basis filters.

$$g_1^x\left(x,y,\sigma_1\right)=\frac{-x}{2\pi\sigma_1^4}\mathrm{e}^{-\frac{\left(x^2+y^2\right)}{2\sigma_1^2}}$$

$$g_1^y\left(x,y,\sigma_1\right)=\frac{-y}{2\pi\sigma_1^4}\mathrm{e}^{-\frac{\left(x^2+y^2\right)}{2\sigma_1^2}}$$

σ_1 is the scale of the gradient estimator.

We need robustness in noise. In order to achieve this, author claimed that response of gradient operator is responsible to achieve the same.The PDF $p(v)$ of the response of the distorted image is calculated alone to the gradient estimator.The critical value $c_1(\sigma_1)$ is a function of 1 that satisfies:

$$\int_{c_1^2}^{\infty} p(u)\, dv = \alpha_p$$

This means that the response bigger than $c_1(\sigma_1)$ is caused not by noise but by edge pixels with the significance level α_p.

$$c_1(\sigma_1) = \frac{\sqrt{-2I_n(\alpha_p)}}{2\sqrt{2\pi\sigma_1^2}} s_n$$

The gradient estimator scale_σ_1 that satisfies

$$\widehat{\sigma_1}(x,y) = inf\{\sigma_1 : r_1^{\theta_M}(x,y,\sigma_1) > C_1(\sigma_1)\}$$

is called the minimum reliable scale where $r_1^{\theta_M}(x,y,\sigma_1)$ is the gradient magnitude in the gradient direction θ_M. σ_1 belongs to some scale octave intervals. To get a more accurate result, we add more intervals in a octave and set $\sigma_1 = \{0.5 * 2^{\frac{i}{3}} \| i = 12, 11, ..., 0\}$The minimum reliable scale is large enough to ensure the response is due to edge pixels while being small enough to minimize errors due to interference from nearby structure. The gradient value at $\sigma_1(x,y)$ is suitable for edge detection. The concept of the minimum reliable scale is the kernel of the Elder-Zucker method.

Chapter 6

Results and Findings

In the Project first find Elder proposes the following to estimate the blur at a particular edge: let:

d = distance in pixels between extrema in 2nd derivative map.

s = minimum reliable scale for second derivative operation.

$blur = \sqrt{\left(\frac{d}{2}\right)^2 - (s^2)}$

The rationale behind this is straightforward. d is an estimate of the sharpness of the edge. However, we cannot estimate this better than the minimum reliable scale, so we correct for that in the estimate. Due to the uncertainty afforded by the minimum reliable scale, we err on the side of less blurring, blurring only those pixels that we are sure need blur.

Steps for finding blur amount:

- Find minimum reliable scale for the gradient operator.
- Find minimum reliable scape for the laplacian operator.
- Find Gaussian smoothing mask in x direction for specified scale.
- Find Gaussian smoothing mask in y direction for specified scale.
- Find partial second derivative mask in x direction.
- Find "cross-partial" second derivative mask.

- Find the magnitude and angle of intensity gradient map in specified image with specified scale. In the event that discretionary marker matrix is given, the matrix will be set to standard derivative all over the place the inclination size surpasses the critical value function of sd1 and took off alone somewhere else and returned.

- create a function which include the information about image. Also scale and agle map of image. And create a matrix for optional marker. This function return the value of laplacian map. On the off chance that given, the optional marker matrix will be set to standard derivative all over the gradient magnitude surpasses the critical value and left alone somewhere else.

- For first derivative and second derivative find the steering function

- Lastly the main function that calls whatever is left of them. It takes two inputs, a picture matrix and a discretionary "noise sigma." It return edge map in delineate unit8 units, the laplacian of Gaussian of the picture, the base reliable scale of every pixel, and an blur evaluation at the edge focuses .

- Then create the graph number of pixels versus blur amount.

Figure 6.1 is the original image and take two image patches from original image then patches converted into gray scale images after converting find the result number of pixel versus the blur amount of pixel, figure 6.4 and figure 6.5 and show the consistency of blur amount and easily define these image is not forged.

Figure 6.1: Result 1: Original Image

Figure 6.2: Result 1.1: Original image patches

Figure 6.3: Result 1.2: Original image patches

- In Figure 6.6 , 6.10 and 6.12 are the forged images and find the two patches blur amount and plotted graph number of pixel versus blur amount of its pixel then easily show the inconsistency of blur in figure 6.9 , 6.11 and 6.13. [Note: Green dot is denoted the First patch blur amount and red dot is denoted the second patch blur amount]

- In figure 6.14 we choose patches from image is not same distance of camera but choose image from different distance from camera so it is not give appropriate result and showing inconsistency of blur amount in figure 6.15 and showing image is forged but originally image is not forged.

- In figure 6.16 we choose patches from image is same distance of camera and create a graph based on number of pixel and blur amount . Easily show inconsistency of blur amount in figure 6.17 and showing image is forged.

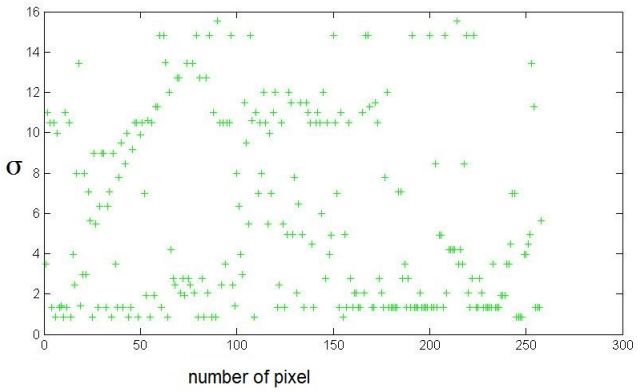

Figure 6.4: Result 1.3: Graph

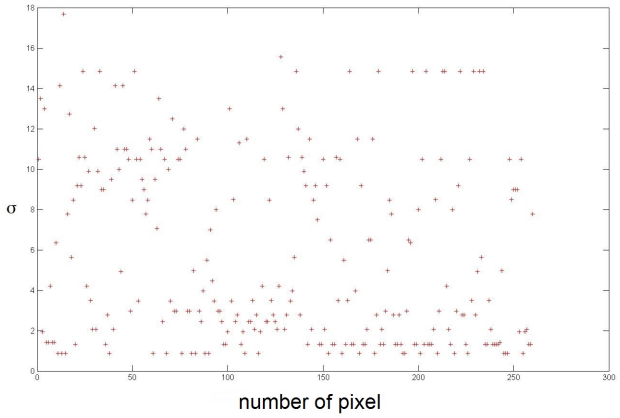

Figure 6.5: Result 1.4: Graph

Figure 6.6: Result 2: Original Image

Figure 6.7: Result 2.1: Original image patches

Figure 6.8: Result 2.2: Original image patches

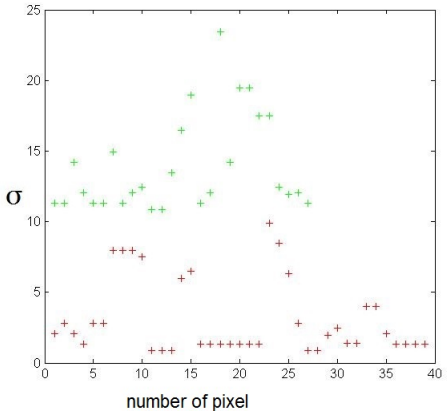

Figure 6.9: Result 2.3: Graph

Figure 6.10: Result 3: Original image

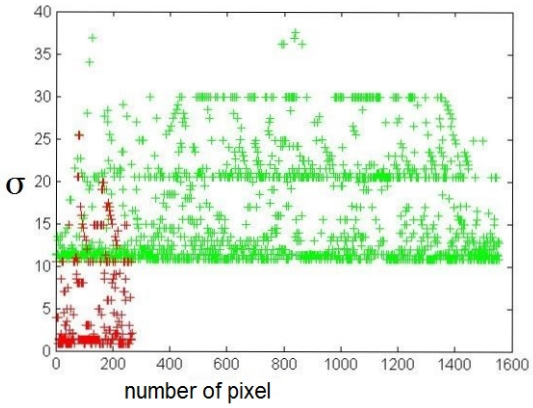

Figure 6.11: Result 3.1: Graph of two patches blur amount

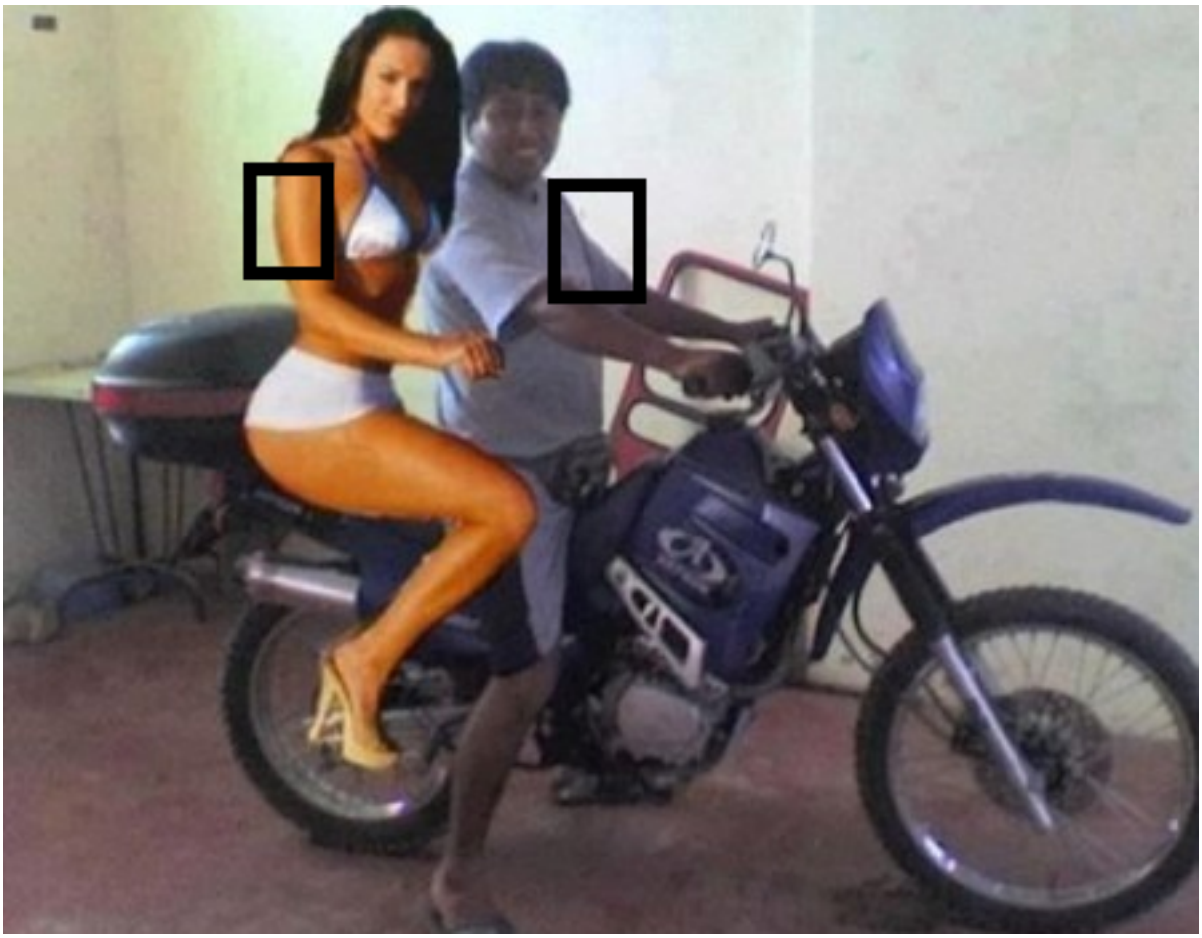

Figure 6.12: Result 4: Original image

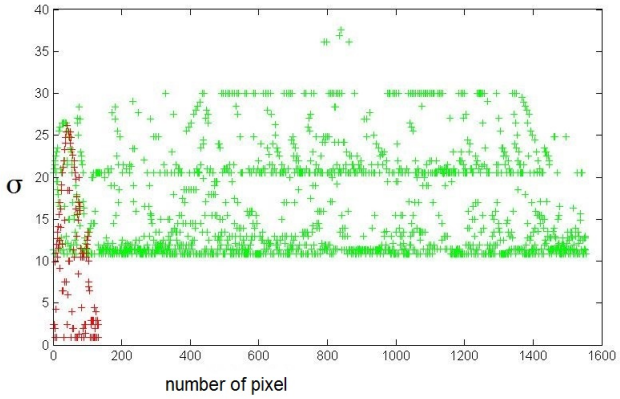

Figure 6.13: Result 4.1: Graph of two patches blur amount

Figure 6.14: Result 5: Original image

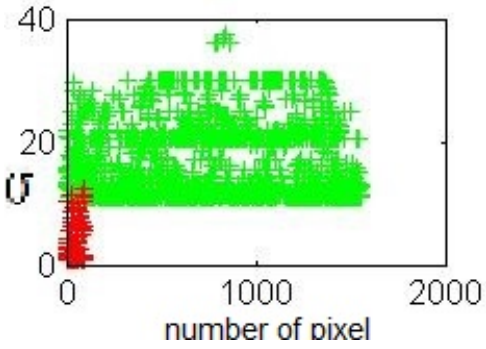

Figure 6.15: Result 5.1: Graph of two patches blur amount

Figure 6.16: Result 6:Forged Image

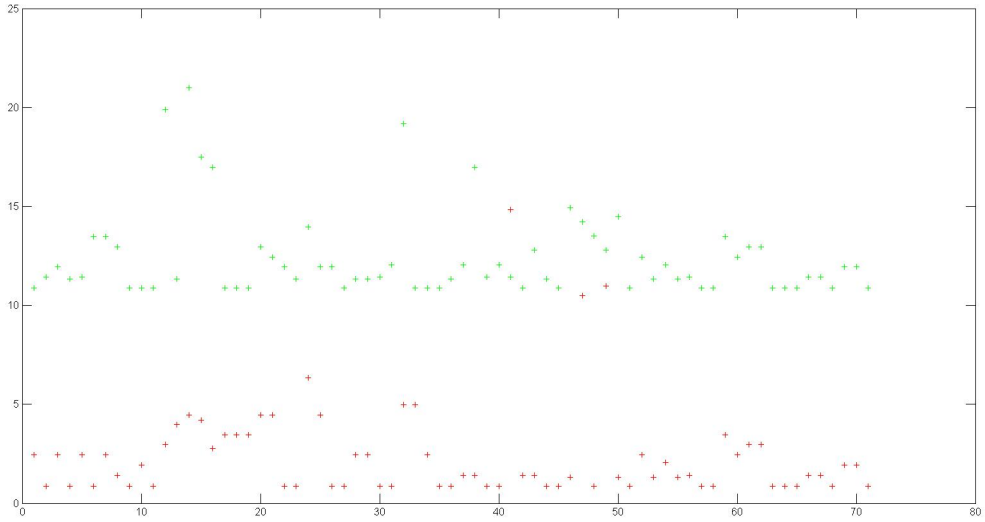

Figure 6.17: Result 6.1: Graph of two patches blur amount

Chapter 7

Conclusion

In this thesis, I have presented the blur amount of image's patch.we cannot estimate this better than the minimum reliable scale, so we correct for that in the estimate. Due to the uncertainty afforded by the minimum reliable scale, we error on the side of less blurring, blurring only those pixels that we are sure need blur. Now Next step will find the result based on the graph which is radius that defines the amount of defocus associated with the depth of the point in the scene and the pixel. Many images are used for the result and finally conclude many point from this passive image forgery detection technique. In the original image if we choses the patches from same distance then the blur amount of the pixel in edge will be consistency and we show first image in our result. Also if we select two patches from different distance then the graph number of pixel and blur amount will be inconsistency so result is not appropriate else image is original. In forged image i experiment this technique on many images and we can easily show the inconsistency between two image patches blur amount.

Bibliography

[1] Hary Farid "Image Forgery Detection", IEEE SIGNAL PROCESSING magazine, March-2009, pp 16-25.

[2] Debevec: Rendering Synthetic Objects into Real Scenes: Bridging Traditional and Image-based Graphics with Global Illumination and High Dynamic Range Photography, Proc. of SIGGRAPH 98, pp. 189198, 1998.

[3] Unger, A. Wenger, T. Hawkins, A. Gardner and P. Debevec: Capturing and Rendering with Incident Light Fields, Proc. of 14th Eurographics workshop on Rendering, pp. 141149, 2003.

[4] Kanbara and N. Yokoya: Real-time Estimation of Light Source Environment for Photorealistic Augmented Reality., Proc. of 17th IAPR Int. Conf. on Pattern Recognition (ICPR2004), pp. 911914, 2004.

[5] Fischer, D. Bartz and W. Strasser: Stylized Augmented Reality for Improved Immersion, Proc. of IEEE Virtual Reality 2005 (VR05), pp. 195202, 2005.

[6] Haller, F. Landerl and M. Billinghurst: A Loose and Sketchy Approach in a Mediated Reality Environment, GRAPHITE 05: Proc. of 3rd Int. Conf. on Computer Graphics and Interactive Techniques in Australasia and South East Asia, pp. 371379, 2005.

[7] Kolb, D. Mitchell and P. Hanrahan: A Realistic Camera Model for Computer Graphics, Proc. of SIGGRAPH 95, pp. 317324, 1995.

[8] Asada and M. Baba: A Unified Camera Model of Zoom, Focus and Iris Parameters for Camera-Calibrated Computer Graphics, Proc. of 6th Int. Conf. on Computer Graphics and Imaging, pp. 101106, 2000.

[9] E. H. B. Smith: Scanner Parameter Estimation Using Bilevel Scans of Star Charts, Proc. of 6th Int. Conf. on Document Analysis and Recognition (ICDAR 2001), pp. 11641168, 2001.

[10] A. N. Rajagopalan and S. Chaudhuri: An MRF Model-Based Approach to Simultaneous Recovery of Depth and Restoration from Defocused Images, IEEE Trans. Pattern Anal. Mach. Intell., Vol. 21, No. 7, pp. 577589, 1999.

[11] N. Asada and M. Baba: A Thin Lens Based Camera Model for Depth Estimation from Defocus and Translation by Zooming, Proc. of 15th Int. Conf. on Vision Interface, pp. 274281, 2002.

[12] P. Favaro and S. Soatto: A Geometric Approach to Shape from Defocus, IEEE Trans. Pattern Anal. Mach. Intell., Vol. 27, No. 3, pp. 406 417, 2005.

[13] M. Irani and S. Peleg: Improving Resolution by Image Registration, CVGIP: Graphical Models and Image Processing, Vol. 53, No. 3, pp. 231239, 1991.

[14] S. C. Park, M. K. Park and M. G. Kang: Super-Resolution Image Reconstruction: A Technical Overview, IEEE Signal Processing Magazine, Vol. 20, No. 3, pp. 2136, 2003.

[15] I. Begin and F. P. Ferrie: Blind Super-Resolution Using a Learning- Based Approach, Proc. of 17th IAPR Int. Conf. on Pattern Recognition (ICPR2004), pp. 8589, 2004.

[16] C. Kolb, D. Mitchell and P. Hanrahan: A Realistic Camera Model for Computer Graphics, Proc. of SIGGRAPH 95, pp. 317324, 1995.

[17] S. Elder, J.H.; Zucker. Local scale control for edge detection and blur estimation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(7):699716, July 1998