A COMPONENT ESTIMATION FRAMEWORK FOR INFORMATION FORENSICS

Ashwin Swaminathan, Min Wu and K. J. Ray Liu

Electrical and Computer Engineering Department, University of Maryland, College Park

ABSTRACT

With a rapid growth of imaging technologies and an increasingly widespread usage of digital images and videos for a large number of high security and forensic applications, there is a strong need for techniques to verify the source and integrity of digital data. Component forensics is new approach for forensic analysis that aims to estimate the algorithms and parameters in each component of the digital device. In this paper, we develop a novel theoretical foundation to understand the fundamental performance limits of component forensics. We define formal notions of identifiability of components in the information processing chain, and present methods to quantify the accuracies at which the component parameters can be estimated. Building upon the proposed theoretical framework, we devise methods to improve the accuracies of component parameter estimation for a wide range of forensic applications.

Index Terms – Component forensics, Fisher information, visual sensors.

1. INTRODUCTION

Digital imaging technologies have witnessed tremendous growth in recent decades. The resolution and quality of imaging devices have been steadily improving and such imaging devices as digital still cameras, scanners, video cameras, and camcorders have been used for a large number of day-to-day activities. Digital images and videos captured using such devices have been used in a number of applications from miliary, reconnaissance, and surveillance to free-lance consumer photography. With such rapid growth and widespread usage arises a number of forensic questions related to the origin and the authenticity of digital data. For example, one can readily ask what kinds of hardware and software components as well as their parameters have been employed inside the devices? Given a digital image/video, which imaging sensor or which brand of sensors was used to acquire it? What kinds of legitimate processing and undesired alteration have been applied to the image/video since it leaves the device? *etc.*

In our recent work [1], we propose *component forensics* as a new methodology for forensic analysis. Component forensics aims at finding the algorithms and parameters employed in each component of the digital device. We show that evidence obtained from such component forensic analysis can be used in a number of applications including discovering patent infringement, authenticating image acquisition source, detecting tampering, and in fostering evolutionary studies. When security is compromised, intellectual rights is violated, or authenticity is forged, component forensic methodologies can be employed to reconstruct what have happened to the content to answer who has done what, when, where, and how. In [1], we use the *intrinsic fingerprint* traces left behind in the final digital image by the different components of the imaging device as evidence to estimate the component parameters and give clues to answer such forensic questions. However, as the intrinsic fingerprint traces pass through the different parts of the information processing chain, some of them may be modified or destroyed and some others newly created. Therefore, the goodness of this forensic evidence depend to a great extent on the accuracy at which they can be obtained and this limits their usage. In this paper, we propose a novel theoretical framework for component forensics to quantify the accuracies at which the intrinsic fingerprints and the component parameters can be estimated. We develop formal notions of identifiability of components and investigate fundamental performance bounds. Building upon this theoretical framework, we devise methods to improve the accuracies of component parameters for a wide range of forensic applications.

While a growing amount of recent research has been devoted to the security and protection of multimedia information (e.g. via encryption, hashing, and watermarking), forensic research on digital visual devices and their outputs is still in its infancy. Related to the emerging image forensics, there is only a handful amount of prior art, which mostly falls in two categories. The first group of prior art on image forensics concerns image acquisition forensics to identify the source of the image to identify if the image is produced via a digital camera, scanner, or generated using computer graphics [1, 2, 3]; and going one step further to identify the camera brand/model/set [1, 4, 5] or the scanner brand/model [6] that was used to capture the picture. In the second group of prior art, there are a few recent works targeted at finding some specific type of post-processing operations that occurs after an image has been captured by a camera and employ such analysis to detect tampering. Different kinds of post-camera processing operations such as resampling [7], lighting, luminance, brightness change [7], and JPEG compression [8] have been modelled and the estimated parameters have been used for forensic analysis. While all these works provide techniques to estimate the parameters of many types of in-camera and post-camera processing, they do not provide a theoretical framework to study forensics; and to our best knowledge, this work is the first one to provide a generalized theoretical framework for information forensics to foster systematic analysis that is widely applicable to a large number of digital devices.

The paper is organized as follows. The proposed theoretical analysis framework is described in Section 2. In Section 3, we illustrate this framework with a particular example from digital cameras and present methods to improve component estimation accuracies. Final conclusions are drawn in Section 4.

2. PROPOSED THEORETICAL ANALYSIS FRAMEWORK

In this section, we introduce a theoretical framework for component forensics and examine the conditions under which the parameters of a component can be estimated accurately. We quantify the accuracy of estimation in terms of *bias* and *variance* of the estimator and derive performance bounds based on Fisher Information. We first review Fisher information in Section 2.1 and then introduce the theoretical formulation in Section 2.2.

Email contact: {ashwins, minwu, kjrliu} @eng.umd.edu.

2.1. Fisher Information and Cramer-Rao Lower Bound

Fisher information is the amount of information that an observable random variable Z carries about an unobservable parameter θ. It is mathematically given by

$$\mathcal{I}(Z,\theta) = E_\theta \left\{ \left[\frac{\partial}{\partial \theta} \ln f(Z|\theta) \right]^2 \right\}, \quad (1)$$

where $f(Z|\theta)$ denotes the probability density function (pdf) of Z conditioned on the value of the parameter to be estimated θ, and the notation E_θ denotes that the expectation is performed conditioned on the value of the parameter θ. The significance of the Fisher information is given by the *Cramer-Rao* lower bound (CRLB). According to the CRLB, the average estimation error given an estimator $\hat{\theta}(Z)$ is lower bounded by

$$E_\theta(\hat{\theta}(Z) - \theta)^2 \geq \frac{\left[1 + \frac{\partial}{\partial \theta} b(\hat{\theta}, \theta)\right]^2}{E_\theta \left\{ \left[\frac{\partial}{\partial \theta} \ln f(Z|\theta) \right]^2 \right\}} + b(\hat{\theta}, \theta)^2, \quad (2)$$

where $b(\hat{\theta}, \theta) = E_\theta(\hat{\theta}(Z)) - \theta$ denotes the *bias* of the estimator. If the estimator, $\hat{\theta}(Z)$, is unbiased, $b(\hat{\theta}, \theta) = 0$ and (2) reduces to $E_\theta(\hat{\theta}(Z) - \theta)^2 \geq \mathcal{I}(Z,\theta)^{-1}$, suggesting that the variance of the estimator is lower bounded by the inverse of Fisher information.

2.2. Theoretical Analysis using Fisher Information

We define a *component* as the basic unit of information processing to facilitate theoretical analysis. For instance, the color filter array, color interpolation algorithms, and white balancing operations can be considered as different components in a digital camera. Each of these components can employ different kinds of algorithms (and/or parameters) in each instantiation of the device, and such differences can be employed for forensic analysis; for instance, to build robust camera identifiers to determine the brand/make of the camera used to capture the digital image [1].

Component forensics refers to a set of techniques to estimate the parameters of the components in various parts of the information processing chain. Component forensic analysis can be classified into three main categories, based on the nature of the available evidence. In *intrusive forensics*, a forensic analyst has access to the device in question and can disassemble it and carefully examine every part. In *semi non-intrusive forensics*, the analyst has access to the device as a black box and can design appropriate inputs to the device and collect the corresponding output data for analyzing the processing techniques and parameters of the individual components. In the *completely non-intrusive forensics* scenario, the forensic analyst is provided only with some sample data produced by the device and does not have access to or other knowledge about the device.

To facilitate theoretical analysis, let $\Re_x$ denote a super-set of all possible inputs that can be given to the k^{th} component $\mathcal{C}_k$, and let $\Re_y$ contain the corresponding outputs. Without loss of generality, let $x \in \Re_x$ be the input and $y \in \Re_y$ denote the corresponding output. Now, we have the following definitions:

Definition The parameter θ_k of a component $\mathcal{C}_k$ can be estimated *intrusively* with an average error $\epsilon_k(x)$ if the best estimator, $\hat{\theta_k}(y,x)$, of the parameter gives $\epsilon_k(x) = E_{\theta_k}(\hat{\theta_k}(y,x) - \theta_k)^2$, where

$$\epsilon_k(x) = \frac{\left[1 + \frac{\partial}{\partial \theta_k} b(\hat{\theta_k}, \theta_k)\right]^2}{E_{\theta_k} \left\{ \left[\frac{\partial}{\partial \theta_k} \ln f(y|x,\theta_k) \right]^2 \right\}} + b(\hat{\theta_k}, \theta_k)^2. \quad (3)$$

From the CRLB, it can be shown that any other estimator $\mathcal{T}(y,x)$ of the parameter θ_k cannot provide error values lower than $\epsilon_k(x)$, *i.e.*, $E_\theta\left((\mathcal{T}(y,x) - \theta_k)|x\right)^2 \geq \epsilon_k(x)$.

If the forensic analyst is not allowed to break open the device, then he/she can either do semi non-intrusive or completely non-intrusive analysis depending on the availability of the device. In this case, we may extend the definition to study multi-component devices. Let a device $\mathcal{D}$ with N_c components be represented as $\mathcal{D} = \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{N_c}\}$, and let $\phi = [\theta_1, \theta_2, \ldots, \theta_{N_c}]^T$ denote set of the parameters of all the N_c components in the device. We may now define the following:

Definition The parameter set ϕ of the device $\mathcal{D}$ can be estimated *semi non-intrusively* with an average error $\underline{\epsilon}_s(x)$ if the best estimator, $\hat{\phi}(y,x) = [\hat{\theta_1}(y,x), \hat{\theta_2}(y,x), \ldots, \hat{\theta_{N_c}}(y,x)]^T$, of the parameter set ϕ gives $\underline{\epsilon}_s(x) = E_\phi(\hat{\phi}(y,x) - \phi)^2$ where

$$\underline{\epsilon}_s(x) = \left(\frac{\partial}{\partial \phi^T} \mathbf{b}_s(\hat{\phi}, \phi) \right) \mathcal{I}_s(x,\phi)^{-1} \left(\frac{\partial}{\partial \phi^T} \mathbf{b}_s(\hat{\phi}, \phi) \right)^T + \mathbf{b}_s(\hat{\phi}, \phi)\mathbf{b}_s(\hat{\phi}, \phi)^T. \quad (4)$$

Here, $\mathbf{b}_s(\hat{\phi}, \phi) = E_\phi(\hat{\phi}(y,x)) - \phi$ represents the bias term, and $\mathcal{I}_s(x,\phi)$ denotes the Fisher information matrix with its $(i,j)^{\text{th}}$ element given by $\mathcal{I}_s^{ij}(x,\phi) = E_\phi\left[\frac{d}{d\theta_i} \ln f(y|x,\phi) \frac{d}{d\theta_j} \ln f(y|x,\phi) \right]$.

As can be seen from (4), the accuracy of parameter estimation depends on the choice of the input to the system and can be improved by designing better inputs. Motivated by this observation, we define a notion of an *ideal* input, $\hat{x}$, as the one that minimizes the average error in parameter estimation, *i.e.*, $\hat{x} = \arg\min_{x \in \Re_x} \underline{\epsilon}_s(x)$, and therefore the lowest error that can achieved via semi non-intrusive analysis is given by $\underline{\epsilon}_s = \underline{\epsilon}_s(\hat{x})$.

Similarly, we may also define the best estimator for non-intrusive forensics as in (4). However, in this scenario, the Fisher Information and the bias terms would not depend on the input x directly as the analyst does not have access to the input. If the estimator is unbiased as is often the case for such camera components as color interpolation and white balancing, the bias terms become zero and therefore the error terms $\underline{\epsilon}_s(x)$ and $\underline{\epsilon}_n$ (corresponding to non-intrusive analysis) depend only on the Fisher information as

$$\underline{\epsilon}_s(x) = \mathcal{I}_s(x,\phi)^{-1}, \quad \underline{\epsilon}_n = \mathcal{I}_n(\phi)^{-1}. \quad (5)$$

We may now establish the following results:

Theorem 1: For an unbiased estimator, the component parameter estimation errors obtained via intrusive analysis, $\underline{\epsilon}_i$, is lower than that obtained via semi non-intrusive analysis, $\underline{\epsilon}_s$; and further $\underline{\epsilon}_s$ is lower than the average estimation errors achieved using completely non-intrusive studies, $\underline{\epsilon}_n$. Thus, we have $\underline{\epsilon}_i \leq \underline{\epsilon}_s \leq \underline{\epsilon}_n$ where ϕ represents the device parameter set.

Proof: Here, we show the proof of $\underline{\epsilon}_s \leq \underline{\epsilon}_n$ for a single component system (where $\phi = \theta$) and the analysis can be extended to devices with multiple components and further to show that $\underline{\epsilon}_i \leq \underline{\epsilon}_s$. Let us define

$$Q = \frac{\partial}{\partial \phi} \ln f(y|\hat{x},\phi) - \frac{\partial}{\partial \phi} \ln f(y|\phi),$$
$$= \frac{1}{f(y|\hat{x},\phi)} \left(\frac{\partial}{\partial \phi} f(y|\hat{x},\phi) - \frac{f(y|\hat{x},\phi)}{f(y|\phi)} \int_{\Re_x} \frac{\partial}{\partial \phi} f(y|x,\phi) p(x) \mathrm{d}x \right)$$

where $p(x)$ represents the pdf of the input x over the space $\Re_x$. We now define $\Re_x^+$ and $\Re_x^-$ as the set of points in $\Re_x$ such that $\frac{\partial}{\partial \phi} f(y|x,\phi) \geq 0$ and $\frac{\partial}{\partial \phi} f(y|x,\phi) < 0$, respectively, and let $p_{max} = \max_{x \in \Re_x} p(x)$. Then, we have

$$Q \geq \frac{1}{f(y|\hat{x},\phi)} \left[\frac{\partial}{\partial \phi} f(y|\hat{x},\phi) + \frac{f(y|\hat{x},\phi)}{f(y|\phi)} \int_{\Re_x^+} \frac{\partial}{\partial \phi} f(y|x,\phi) \times (p_{max} - p(x)) \mathrm{d}x \right]. \quad (6)$$

The second term in (6) is non-negative for all x since $p(x) \leq p_{max}$, and by choosing $\hat{x} \in \Re_x^+$, the first term also becomes non-negative. Thus, there exists and input $\hat{x}$ such that $Q \geq 0$. Squaring and taking expectations, we get $\mathcal{I}_s(\hat{x},\phi) \geq \mathcal{I}_n(\phi)$ which gives the desired result.

Corollary: The proof of *Theorem 1* also implies the existence of an ideal input for semi non-intrusive forensics; and further the ideal input, $\hat{x}$, is an element of the subspace $\Re_x^+$.

Theorem 2: The equalities in Fisher information $\mathcal{I}_s(x,\phi) = \mathcal{I}_n(\phi)$ for a given input x is attained only when $f(x|y,\phi)$ is independent of ϕ.

Proof: The proof follows from the definitions of Fisher information and it can be shown that

$$\mathcal{I}_s(x,\phi) = \mathcal{I}_n(\phi) + E_\phi \left\{ \left(\frac{\partial}{\partial \phi} \ln(f(x|y,\phi)) \right)^2 + \left(\frac{\partial}{\partial \phi} \ln(f(y|\phi)) \right) \left(\frac{\partial}{\partial \phi} \ln(f(x|y,\phi)) \right) \right\}, \quad (7)$$

with the equality is attained only when $\frac{\partial}{\partial \phi} \ln(f(x|y,\phi)) = 0$, which gives the desired result and completes the proof. This theorem provides a scenario when the best estimation accuracy obtained via completely non-intrusive analysis equals the accuracies attained via semi non-intrusive studies.

3. CASE STUDIES WITH DIGITAL CAMERAS

In this section, we illustrate the proposed theoretical framework using illustrative examples from digital cameras and the proposed techniques can be extended to other kinds of digital devices.

3.1. Image Capture Process in Digital Cameras

The dashed box in Fig. 1 shows the image capture process in digital cameras. The input light from a real-world scene passes through lens and optical filters, and is finally recorded by sensor arrays. Most commercial digital cameras and camcorders employ a color filter array (CFA) to sample the real-world scene [9]. The CFA consists of an array of color filters, typically a pattern tiled with 2×2 cells of R/G/B filters. These filters allow the sensors to better capture the corresponding color of the real-world scene at its pixel location. The remaining color values of the pixel are interpolated from the neighborhood [9]. After interpolation, the three images each corresponding to the red, green and blue components go though a post-processing stage. Color corrections such as white balancing are done in this stage, and the image or the image sequence may be lossily compressed (e.g. via JPEG or MPEG) to reduce storage space.

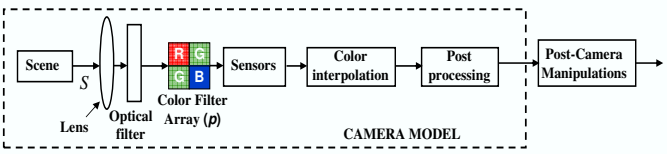

Fig. 1. Image Capturing Model in Digital Cameras showing its individual components

To cope with the dependency among multiple interconnected components inside a camera, in our recent work [1], we have developed a robust and non-intrusive algorithm that makes inference from output images to jointly estimate such *in-camera* processing operations as the color filter array and color interpolation parameters. In [10], we show that most post-camera processing operations can be modelled as a separate component and its parameters can be estimated to identify different types of tampering and steganographic embedding operations.

3.2. Mathematical Model for In-Camera Processing

In this subsection, we present a mathematical model for in-camera processing to demonstrate the applicability of the proposed theoretical analysis framework to study camera components. We consider color interpolation as a specific example and the techniques developed can be extended to other components. Most cameras of different brands/models employ a different algorithms for color interpolation and therefore estimating the interpolation parameters provides very useful information to build a robust camera identifier [1, 4]. In our recent work [1], we show that color interpolation can be well approximated by fitting linear models in three different regions of the image corresponding to smooth and edge regions (with significant horizontal and vertical gradients). Thus, color interpolation in each region and color can be approximated as

$$y(k,l) = \sum_{m=-\lfloor N_h/2 \rfloor}^{\lfloor N_h/2 \rfloor} \sum_{n=-\lfloor N_h/2 \rfloor}^{\lfloor N_h/2 \rfloor} h(m,n) x(k-m, l-n), \quad (8)$$

where x and y represent the pixel values in the input and output images in the chosen region of the image, and h denote the corresponding filter coefficients of size $(N_h \times N_h)$.

The color interpolation parameters h can be estimated given the CFA sampling pattern. To estimate h, we obtain the locations of the set of pixels that are interpolated and those that are directly obtained from the sensor and construct a set of linear equations

$$\begin{bmatrix} y(1,1) \\ y(1,2) \\ y(1,3) \\ y(1,4) \\ \vdots \\ y(W,H) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & \dots \\ h(0,1) & 0 & h(0,-1) & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ h(0,3) & 0 & h(0,1) & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \\ 0 & 0 & 0 & 0 & \dots \end{bmatrix} \begin{bmatrix} x(1,1) \\ x(1,2) \\ x(1,3) \\ x(1,4) \\ \vdots \\ x(W,H) \end{bmatrix}, \quad (9)$$

where W and H denote the width and the height of the image. We note that the values $\{y(1,1), y(1,3), y(1,5), \dots\}$ are obtained directly from the camera input and the remaining intermediate pixel values $\{y(1,2), y(1,4), y(1,6), \dots\}$ are interpolated using the filter. As can be seen from the set of linear equations, with the knowledge of the CFA, the output y gives complete information

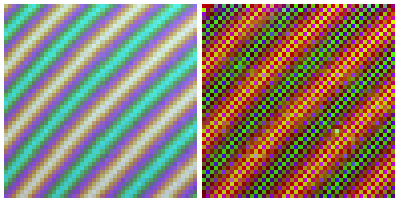

Fig. 2. Digitally zoomed versions of a 32×32 part in the original and optimized input patterns

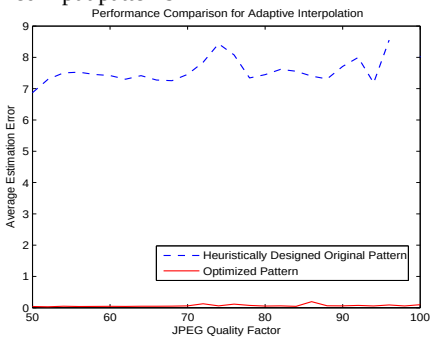

Fig. 3. Average Estimation Error for Semi Non-Intrusive Forensics as a function of JPEG quality factor

about the input as $\{x(1,1) = y(1,1), x(1,3) = y(1,3), \ldots\}$; and therefore $f(x|y,\theta)$ is independent of θ satisfying the conditions in *Theorem 2* to suggest that $\underline{\epsilon}_s(x) = \underline{\epsilon}_n$. This set of equations can be solved non-intrusively or semi non-intrusively by an unbiased least squares method to estimate the component parameters.

3.3. Optimal Pattern Design for Semi Non-Intrusive Forensics

In our recent work on semi non-intrusive forensics [11], we present a heuristic approach to design a good input to estimate the parameters of such camera components as color interpolation and white balancing, and show that the accuracies in estimating the component parameters can be improved via such an approach. In this subsection, we show an application of the proposed theoretical analysis framework to optimize this input pattern to obtain *ideal* inputs.

We optimize the input pattern for semi non-intrusive forensics by solving a minimization problem that minimizes the parameter estimation accuracies, $\underline{\epsilon}_s(x)$. The input-output relationship of color interpolation in (9) can be re-written to obtain equations of the form $Y = X\theta + n$, where $\theta = [h(-N_h, -N_h), \ldots, h(N_h, N_h)]^T$. Further, the estimation error for an input x can be shown to be equal to the inverse of the SNR, *i.e.*, $\underline{\epsilon}_s(x) = \sigma_n^2 (X^T X)^{-1}$ where σ_n^2 is the variance of the additive noise. An iterative technique based on gradient-descent algorithm can then be employed to minimize the cost function $\underline{\epsilon}_s(x)$ and to optimize the pixel values of the input pattern.

In Fig. 2, we show the results of the optimization algorithm for a 32×32 part the original input along with the optimized version for comparison. To test the goodness of the designed pattern and the optimized pattern for estimating the cameras' color interpolation parameters, we first interpolate both the original and the optimized images shown in Fig. 2 using different kinds of adaptive interpolation algorithms such as gradient based and adaptive color plane. We then post-process the interpolated images by JPEG compressing them under different quality factors; and finally re-estimate the interpolation coefficients from the compressed versions. Fig. 3 shows the estimation error as a function of the JPEG quality factor for both the heuristically designed input and the optimized input image. The figure shows the average error is significantly lower for the case of the optimized pattern compared with the original pattern. This illustration suggests that the theoretical framework can be employed to design ideal input patterns to estimate the color interpolation parameters with improved robustness to post-interpolation operations such as JPEG compression.

4. CONCLUSIONS

In this paper, we develop a novel theoretical model for information forensics to answer what components and processing operations are identifiable and what are not. The proposed theoretical foundations provide a basis to analyze different parts of the information processing chain in a systematic way. We define formal notions of identifiability of components under different scenarios; and quantify the accuracies at which the component parameters can be estimated in each case using Fisher information as a criterion. We show that intrusive forensics gives superior estimation accuracies over semi non-intrusive forensics and this is better than completely non-intrusive scenario. We then employ the theoretical foundation to design ideal inputs; and show that the estimation accuracies can be improved via such an approach. The proposed theoretical model can also be extended to study post-camera processing operations such as tampering and steganographic embedding as a separate component; and provide a solid foundation for information forensics to answer a number of forensic questions related to who has done what to the content, when and how.

5. REFERENCES

[1] A. Swaminathan, M. Wu, and K. J. Ray Liu, "Non-Intrusive Component Forensics of Visual Sensors Using Output Images," in *IEEE Trans. on Info. Forensics and Security*, vol. 2, no. 1, pp. 91-106, Mar 2007.

[2] T-T. Ng, S-F. Chang, J. Hsu, L. Xie, M-P. Tsui, "Physics-motivated features for distinguishing photographic images and computer graphics," *ACM Multimedia*, Singapore, Nov 2005.

[3] A. C. Popescu and H. Farid, "Exposing Digital Forgeries in Color Filter Array Interpolated Images," *IEEE Trans. on Signal Processing*, vol. 53, no. 10, part 2, pp. 3948–3959, Oct 2005.

[4] S. Bayram, H. T. Sencar, and N. Memon, "Improvements on Source Camera-Model Identification Based on CFA Interpolation," *Proc. of the WG 11.9 Intl. Conf. on Digital Forensics*, Orlando, FL, Jan 2006.

[5] J. Lukas, J. Fridrich, and M. Goljan, "Determining Digital Image Origin Using Sensor Imperfections," *Proc. of the SPIE, Security, Stego. and Wmk of Multimedia Contents VII*, vol. 5681, pp. 249–260, Jan 2005.

[6] N. Khanna, A. K. Mikkilineni, G. T. C. Chiu, J. P. Allebach, and E. J. Delp, "Scanner Identification Using Sensor Pattern Noise," *Proc. of the SPIE, Security, Stego and Wmk of Mult. Contents IX*, Feb 2007.

[7] A. C. Popescu and H. Farid, "Statistical Tools for Digital Forensics," *Intl. Workshop on Info. Hiding*, Toronto, Canada, 2004.

[8] J. Lukas and J. Fridrich, "Estimation of Primary Quantization Matrix in Double Compressed JPEG Images," *Proc. of the DFRWS*, Aug 2003.

[9] J. Adams, "Interaction between Color Plane Interpolation and Other Image Processing Functions in Electronic Photography," *Proc. of the SPIE, Cameras and Systems for Electronic Photography ad Sci. Imaging*, vol. 2416, pp. 144–151, Feb 1995.

[10] A. Swaminathan, M. Wu, and K. J. Ray Liu, "Image Tampering Identification Using Blind Deconvolution," *Proc. of the ICIP*, Oct 2006.

[11] A. Swaminathan, M. Wu, and K. J. R. Liu, "Optimization of Input Pattern for Semi Non-Intrusive Component Forensics of Digital Cameras," *Proc. of the ICASSP*, Honolulu, HI, Apr 2007.