Forensic Analysis of Digital Imaging Devices

Christine McKay
Advised by: Ashwin Swaminathan, Hongmei Gou, and Prof. Min Wu
MERIT Program, Electrical and Computer Engineering Department
University of Maryland, College Park
Email: cemckay@umd.edu

***Abstract* - Non-intrusive component forensics involves identifying algorithms and parameters of a device based on its output data alone. This project extends several of these techniques from standalone digital cameras to cell phone cameras. Methods used include estimating a device's color interpolation coefficients and noise feature parameters. Robustness to post-camera operations such as digital zoom and JPEG compression is also examined. This research applies to law enforcement and intelligence operations in differentiating between camera-, scanner-, and computer-generated images and determining the brand/model of the device used to capture an image. Further, this research is useful in identifying image tampering and patent infringement.**

I. INTRODUCTION

Cell phones with embedded cameras and regular standalone digital cameras have become quite ubiquitous in today's society, and in some ways they are equally as controversial. For example, it is possible and common for one to take a photo surreptitiously using a cell phone, seemingly talking or typing or reading a text message, while in actuality snapping a picture. For many, this is viewed as an invasion of privacy and a risk to secure information, since the picture-taker may not have innocent intentions. For precisely this reason, some countries, such as South Korea, have enacted laws requiring that cell phone cameras produce a sound when a picture is taken[1]. In other ways, the widespread presence of cameras, especially cell phone cameras, has proved beneficial to society. While it is common to carry a cell phone, it is far less common to carry a standard camera under normal circumstances, as the portability of cell phones is very convenient. This can be helpful, for example, by allowing eyewitnesses of a crime to take pictures to provide evidence to authorities. Recently, the cell phone video captured by a Virginia Tech student on April 26, 2007 allowed the world to view the aftermath of the tragic events there. Figure 1 shows the expected continued growth in sales of standalone cameras and of cell phone cameras (which will soon top 1 billion per year), as well as scanners. While the digital camera is often useful and convenient, a number of forensic issues are raised by the standalone camera and cell phone camera technologies.

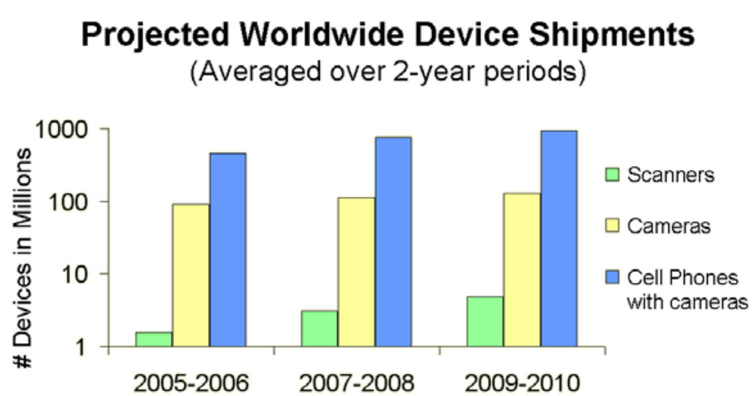

Figure 1. Projected growth of sales of imaging devices worldwide[2]

Non-intrusive component forensics aims to identify distinguishing features of an image acquisition device using its output data alone. In this project, data regarding color interpolation coefficients and noise features are obtained from pictures from five different models of cell phones, five models of standalone cameras, and four models of scanners, in order to create a model for determining which type of device was used to capture a new image. Once the device is known, these methods can be extended to determining which brand and model of device was used to capture the image.

The importance of applying non-intrusive component forensics to imaging devices is especially noteworthy in the detection of image tampering and in its benefits to law enforcement officials, as well as detecting possible patent infringement. A common method of image tampering is known as the cut-and-paste method, which involves putting together parts of two or more different pictures into one picture and passing it off as an original picture. This is easily done using software, and if done well is not detectable just using one's eye. The methods described in this paper are able to detect which parts of a tampered image were taken by which type of device and its brand and model, proving that the image is not an original. There are several known instances of journalists doctoring photos before publication, a type of fraud which should ideally be detectable. In addition, the field of non-intrusive component forensics can be helpful to law enforcement, as in the event that a photo with sensitive information appears, it may be possible to ascertain the type and model of the acquiring device, and from there, get closer to knowing the original taker of the photo. Patent infringement can be detected in the case that two devices are so similar that the images they produce have very similar extracted features. In classifying these images, one device’s image could easily be classified as belonging to the other device, and a large enough incidence of this could point to patent infringement for one of the devices.

The paper is organized as follows. In Section II, we discuss how the image acquisition process differs in cell phone cameras, standalone cameras, and scanners. In Section III, we describe the color interpolation coefficient and noise parameter estimation methods and how they are used to classify images by acquisition device and by the specific camera or scanner model. Detailed simulation results and experiments are presented in Section IV and robustness to JPEG compression and digital zoom are examined in Section V. Some comparisons with prior works are reported in Section VI and final conclusions are drawn in Section VII.

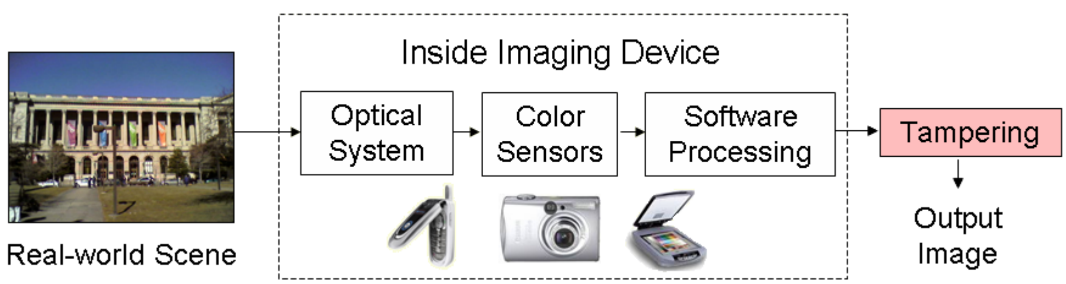

Figure 2. General image acquisition model for scanners and cameras

II. IMAGE ACQUISITION PROCESS

Figure 2 shows the image acquisition process. The light from the scene passes through the lens and the optical filters and is finally recorded by an array of charge coupled device (CCD) detectors. Most scanners use tri-linear CCDs corresponding to red, green, and blue components (as shown in

Figure 3), while digital cameras use a 2-D periodic CCD array, such as the well-known Bayer Color Filter Array (CFA) pattern shown in Figure 4 to sample the real-world scene. Using the tri-linear CCD array along with the line-by-line acquisition mode enabled by the motion system, scanners can directly capture all the three color components of each raster line. On the contrary, digital cameras use a square CCD array to capture the entire 2-D scene in one shot. Therefore, in standalone and cell phone cameras, only one color is obtained for each pixel. An image is captured in cameras through a lens and a two-dimensional CFA pattern. The CFA pattern determines which color is obtained for a given pixel, and the Bayer CFA pattern is by far the most common. This Bayer pattern is a 2x2 square with one red, one blue, and two green pixels; there are twice as many green since luminance is detected best with green. The 2x2 square is replicated many times to create an array representing the entire image. The remaining two colors for any given pixel are estimated through an interpolation process, and in most cases the interpolation algorithm is unique to each model of camera.

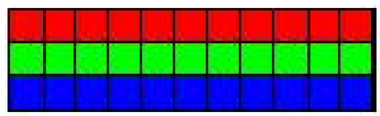

Figure 3. Tri-linear CFA pattern used in Scanners[3]

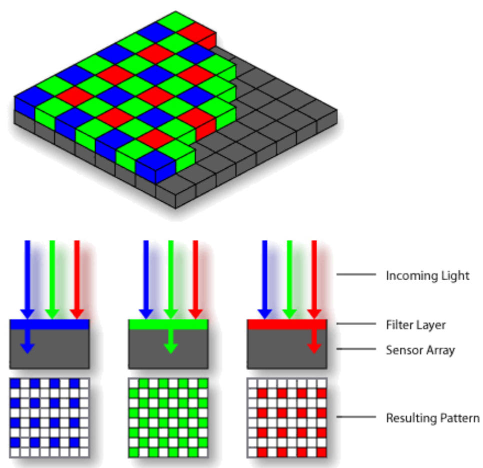

Figure 4. Bayer CFA pattern[4] used in most digital standalone cameras and cell phone cameras

Standalone digital cameras and scanners most commonly use a CCD (charge coupled device) sensor array to record the voltages generated by the light exposure corresponding to a particular color. Cell phones typically use CMOS image sensors for this purpose. CMOS sensors are cheaper, faster, and use much less power than their CCD counterparts, as they combine sensor and processing technologies onto one chip. However, CMOS sensors produce more noise than CCDs.

After color interpolation, the interpolated images pass through a post-processing stage. This stage may include operations such as white-balancing, noise reduction, color correction, and JPEG compression. In standalone cameras, JPEG compression is performed with a quality factor close to 100% to minimize information loss; however, cell phone cameras will often use lower quality by default, in order to keep file size smaller and preserve memory. In the cameras studied, the cell phones used quality factors ranging from 65-85%. For this reason, as well as the extra noise from the CMOS image sensors, picture quality in cell phone pictures lags behind that of standalone cameras. In addition, cell phone cameras typically produce much smaller pictures than standalone cameras (the most common size researched for this paper was 640x480 pixels or 0.3 megapixels). Therefore, forensic methods designed for standalone cameras cannot be directly used by cell phone cameras, and the creation of new methods that successfully include cell phone cameras is the focus of our work.

III. METHODOLOGY

An important goal of non-intrusive component forensics is to verify the authenticity of an image by tracing its origins and examining the possibility of tampering. Acquisition forensics refers to the objective of determining if an image was captured by a camera, cell phone camera, scanner, or was computer generated. This can be important for, as an example, verifying that a photo reportedly captured by a journalist or eyewitness actually originated from a camera and was not created using graphics software. Another forensics field, device identification forensics, aims to determine the brand and model of camera, cell phone, or scanner used to capture an image in question. One application of this is to prove or disprove that each part of an image originates from the same model of camera, if one if looking for evidence of cut-and-paste tampering.

To create a successful identification scheme, one must first find sources of variation among different types of devices and between different models of a device. Once these differences are discovered, they can be extracted and represented as unique features of each device which can be used for identifying the source of an unknown new image. The distinguishing features discussed in this paper are color interpolation coefficients[3,5] and noise features[6]. Since each model of camera uses a different color interpolation method, this can be exploited forensically to help distinguish between various models. The Bayer pattern is assumed, since in previous studies of digital cameras all cameras studied used this CFA pattern. The CFA pattern tells which pixels are original and non-interpolated for each color. The interpolated pixels can then be represented as a linear combination of the neighboring original pixels. The set of equations obtained in this way can be solved to find the estimated interpolation coefficients.

Noise occurs when photoelectrons are created in the imaging device. One example of measurable noise is dark signal non-uniformity, or variations between pixel voltage under conditions of no light. Photo response non-uniformity can be measured as the variations between pixel voltage under light with fixed intensity. There are also other small sources of noise within each device. While the imaging device will attempt to compensate for and reduce noise in the image, some will still exist depending on the specific nature of the sensors and filters used. In noise feature analysis, there are three components – denoising, wavelet, and neighborhood prediction. In denoising, an image is denoised using four different algorithms, and for each one the difference between the original and the denoised image is measured. Next, wavelet analysis decomposes the image into frequency sub-bands to measure observe the effects of noise in the frequency domain. Lastly, the neighborhood prediction algorithm measures error in the prediction of neighboring pixels in smooth regions.[6]

After features are obtained from sample images, the data are classified using a support vector machine (SVM) to identify the source type of the image (whether the image is scanned, camera captured, a cell phone picture, or a computer generated graphics image). In our experiments, we utilized a SVM with a non-linear radial basis function kernel. A specified fraction of images ,usually 85-99% of images, are used for training the SVM, with the remaining images used for testing. In the testing process, the SVM classifies an image into the class into which it lies based on its noise and interpolation feature data and the training that has been completed previously.

IV. SIMULATION RESULTS

In this study, four models of scanners each with 96 sample images, five cell phone cameras models each with 100 images, five standalone cameras models each with 38 images, and 100 computer generated images were included. Since this is a completely non-intrusive study, the sample images were taken in random conditions, without any controlled experimental setup. In this way, the images should simulate real-world data in terms of lighting, color, texture, and subject. Interpolation coefficient estimation and noise feature detection were run on each sample image, with the resulting data put into one large vector for each image. In the first part of this study, 100 images from each type of device (cell phone camera, standalone camera, and scanner) were selected with an equal number from each model, and all CG images were used, to create four classes of 100 images each. 99 random images from each class were used to train the SVM classifier, which is known as the leave-one-out scheme. The one remaining image from each class (4 images total) was used for testing. This was repeated for 100 iterations. The resulting confusion matrices from each iteration are averaged together to produce the final confusion matrix, shown below in Table 1. The (i,j)th element in the table corresponds to the fraction of images from source type-i classified as belonging to source type-j. The main diagonal elements give the percentage of correct identification and the average of the main diagonal elements give the classification accuracy. From the results in Table 1, we find that overall identification accuracy is 93.75%**,** suggesting that the proposed features are good for identifying the source type.

Table 1. Confusion matrix showing source device identification, with an overall accuracy of 93.75%

Device	Cell Phone	Standalone Camera	Scanner	CG
Cell Phone	93%	2%	0	5%
Standalone	1%	98%	1%	0
Scanner	1%	3%	94%	2%
CG	4%	2%	4%	90%

Once an image's source device has been determined, further classification can be performed on the particular brand or model of the device. For scanners, it was found that using the combination of interpolation coefficients and noise feature parameters gave the best results. The confusion matrix for scanners is found in Table 2. The four brands of scanners used were Epson, AcerScan, Canon, and MicroTek. 96 images from each scanner were used. 86 random images from each scanner were chosen for training, with the remaining 10 used for testing. As seen in Table 2, the overall identification accuracy for scanner brand is 96.2%.

Table 2. Confusion matrix showing scanner model identification, with an overall accuracy of 96.2%

Scanner	Epson	AcerScan	Canon	MicroTek
Epson	97.4%	2.6%	0	0
AcerScan	4.2%	90%	4.4%	1.4%
Canon	0	0	97.4%	2.6%
MicroTek	0	0	0	100%

For both standalone cameras and cell phone cameras, using interpolation coefficients alone, rather than a combination of interpolation coefficients and noise features, produced the highest accuracy. The five models of standalone cameras used were Canon A75, FujiFilm s3000, Casio QV-ux2000, Minolta DiMage F100, and Canon PowerShot s410. 38 images from each camera were used, with 37 random images used for training and the one remaining image used for testing. Table 3 gives the results for identification of brand of standalone cameras, which produce an overall identification accuracy of 95%. These results are better than the ones reported in literature[10,11] with average classification accuracies of 84% and 95%, respectively, over a smaller dataset of three camera brands.

Table 3. Confusion matrix showing standalone camera model identification, with an overall accuracy of 95%

Camera	Canon A75	FujiFilm	Casio	Minolta	Canon PowerShot
Canon A75	98%	0	0	0	2%
FujiFilm	0	100%	0	0	0
Casio	0	0	100%	0	0
Minolta	0.5%	2%	5%	87.5%	5%
Canon PS	5%	0	0	5.5%	89.5%

The five models of cell phones cameras studied were Nokia 6102, Motorola V550, Samsung c417, Sony Ericsson w810, and Audiovox CDM-8910. 100 images from each cell phone were studied, of which 90 random images were used for training and the remaining 10 were used for testing. As with the standalone cameras, using interpolation features alone produced the highest accuracy results. Table 4 gives the results for identification of brand of cell phone camera, which produce an overall identification accuracy of 97.7% which is significantly better than state-of-the-art techniques that produce average accuracies close to 92% over four camera models from two different camera brands[12].

Table 4. Confusion matrix showing cell phone camera model identification, with an overall accuracy of 97.7%

Cell Phone	Nokia	Motorola	Samsung	Sony	Audiovox
Nokia	95.8%	0.4%	0	3.8%	0
Motorola	2.8%	97.2%	0	0	0
Samsung	1.2%	0	97.8%	0.2%	0.8%
Sony	2.4%	0	0	97.6%	0
Audiovox	0	0	0	0	100%

An interesting result is that scanner classification performs very well using interpolation features, even though scanners do not use color interpolation. Since scanners use tri-linear color filters at each pixel, each color is known at every pixel and no color estimation is required. Therefore, no patterns would be expected among the relationship between the color values of neighboring pixels. The reasons for these results are currently being investigated. The confusion matrix for classifying by scanner model using interpolation coefficients only is given in Table 5.

Table 5. Confusion matrix showing scanner model identification, with 86 training images out of 96 total images, using color interpolation coefficient data only; overall accuracy is 92%

Scanner	Epson	AcerScan	Canon	MicroTek
Epson	99.2%	0	0.8%	0
AcerScan	1.8%	89.8%	6.8%	1.6%
Canon	2%	5.4%	90.4%	2.2%
MicroTek	0.4%	6%	5.4%	88.2%

V. ROBUSTNESS OF METHODS

In this section, we examine the robustness of the proposed techniques for post camera processing operations such as digital zoom and JPEG compression. As shown in the previous sections, using original, untampered images, the proposed methods used for classification work very well, with 94-98% accuracy on average for device and model identification. The methods were also tested on images that had undergone some kind of tampering, such as additional JPEG compression or resampling. In these cases, we wish to be able to identify the originating device with high accuracy, even though the image has undergone post-processing operations.

Robustness to additional JPEG compression was tested on the cell phone camera images. JPEG is a lossy compression method, meaning that the original image cannot be recovered exactly when decompressed. A quality factor of 0-100 is associated with JPEG compression, with 100 meaning highest quality and therefore largest file size.

For our compression tests, four new groups of cell phone images were created using further JPEG compression with quality factors 90, 80, 70, and 60, respectively. For each of these four groups, interpolation coefficient and noise feature data were collected, to be used in the SVM training and testing. Since some data is lost during compression, it is expected that the original coefficient and noise parameters will be more difficult to detect as accurately, and that there will be less variation between images from different models of camera 90 images were used for training and 10 were used for testing, with 50 iterations for each classification.

In reviewing the results with JPEG compression with quality factor below 100, it was found that the best results came when only some of the features were used. The Sequential Floating Forward Selection (SFFS) algorithm[7] selects a subset of features that are most significant for classification. The minimum redundancy-maximum relevance SFFS method was used to rank the combined noise and interpolation coefficient data so that only the most significant could be used. In the case of the compressed images, using only 88 of the original 516 features produced the highest accuracy. To implement this, only those specific 88 features were used in the SVM training, and only those 88 features were used for the testing images. A possible explanation for why SFFS produces better results in classifying the compressed images but not the original images is that with the compressed images, some of the extracted features may have more redundancy than the original images because some of the original image data has been lost. In addition, it should be noted that since using the SFFS-reduced feature set is more accurate only in identification of the extra-compressed images, but original images get highest accuracy using the full feature set, first a method must be used to determine that an image is JPEG compressed and not an original image.

Tables 6-9 show the identification results using the SFFS-reduced features set on the images compressed with quality factors of 90%, 80%, 70%, and 60%, respectively.

Table 6. Confusion matrix showing cell phone camera identification, with 90% quality additional JPEG compression, producing an identification accuracy of 95.6%

Cell Phone	Nokia	Motorola	Samsung	Sony	Audiovox
Nokia	93.6%	2.6%	0.4%	2%	1.4%
Motorola	3.2%	94.8%	0.2%	0.6%	1.2%
Samsung	3%	1.4%	94.4%	0	1.2%
Sony	2%	0.6%	0	96.4%	1%
Audiovox	0	1.2%	0	0	98.8%

Table 7. Confusion matrix showing cell phone camera identification, with 80% quality additional JPEG compression, producing an identification accuracy of 94.5%

Cell Phone	Nokia	Motorola	Samsung	Sony	Audiovox
Nokia	92%	3.2%	0.6%	2.8%	1.4%
Motorola	4.2%	94%	0	0.6%	1.2%
Samsung	1.4%	4.4%	93.6%	0	0.6%
Sony	3.4%	0.6%	0	94.8%	1.2%
Audiovox	0.6%	1.2%	0	0	98.2%

Table 8. Confusion matrix showing cell phone camera identification, with 70% quality additional JPEG compression, producing an identification accuracy of 94.3%

Cell Phone	Nokia	Motorola	Samsung	Sony	Audiovox
Nokia	91.4%	2.8%	4%	0.8%	1%
Motorola	4.4%	91.6%	0.2%	2%	1.8%
Samsung	3.4%	0.8%	93.2%	1.6%	1%
Sony	2.6%	0.8%	0	96%	0.6%
Audiovox	0.2%	0.6%	0	0	99.2%

Table 9. Confusion matrix showing cell phone camera identification, with 60% quality additional JPEG compression, producing an identification accuracy of 91.0%

Cell Phone	Nokia	Motorola	Samsung	Sony	Audiovox
Nokia	89.4%	4.8%	4.6%	1.2%	0
Motorola	6.4%	89.8%	0.2%	2%	1.6%
Samsung	2.4%	1.8%	94.8%	0.2%	1%
Sony	2.4%	1%	0	96.6%	0
Audiovox	0.8%	9%	0	5.6%	84.6%

Figure 5 demonstrates how as compression quality decreases, the rate of correct identification decreases. However, the lowest accuracy achieved was 91%, which is still very good.

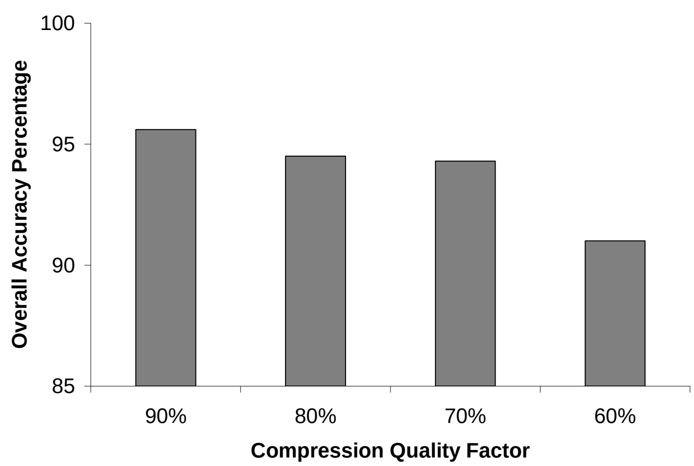

Figure 5. Graph of the overall identification accuracy for the four different compression quality factors tested on cell phone cameras.

Robustness of these methods to digital zoom is also an important and desired element. Depending on the level of zoom, a certain number of pixels are inserted between the original pixels, and interpolation is used to determine the color values of the new pixels. Common methods of interpolation include bilinear, bicubic, and nearest-neighbor. This extra interpolation step makes the original interpolation coefficients very difficult to recover. Therefore, classifying images that were altered with digital zoom yielded unimpressive results. However, classification of images that were upsampled using nearest neighbor interpolation by a factor x, then downsampled by a factor 1/x to produce an image with the same size as the original gave better results, as shown in the tables below. Table 10 shows the results with images upsampled by 1.25 then downsampled by 0.8, with an overall accuracy of 89.2%. Table 11 shows the results with images upsampled by 2 then downsampled by 0.5, with an overall accuracy of 91.5%. 90 images were used in training, 10 images were used in testing, with 50 iterations averaged to create the confusion matrices.

Table 10. Confusion matrix showing cell phone camera identification, with images upsampled by 1.25 then downsampled by 0.8; overall identification accuracy is 89.2%

Cell Phone	Nokia	Motorola	Samsung	Sony	Audiovox
Nokia	91.6%	2.6%	0.6%	3.8%	1.4%
Motorola	4%	91.8%	0	2.8%	1.4%
Samsung	4%	1.6%	92.6%	0.8%	1%
Sony	9.8%	4.6%	0	84%	1.6%
Audiovox	2.6%	4%	0	7.6%	85.8%

Table 11. Confusion matrix showing cell phone camera identification, with images upsampled by 2 then downsampled by 0.5; overall identification accuracy is 91.5%

Cell Phone	Nokia	Motorola	Samsung	Sony	Audiovox
Nokia	93%	3.2%	0	2.4%	1.4%
Motorola	0.8%	94.8%	0.2%	1.8%	2.4%
Samsung	5.8%	2.6%	88.6%	1.8%	1.2%
Sony	7.4%	1%	0	91.4%	0.2%
Audiovox	3%	2.6%	0	4.8%	89.6%

To utilize the methods used in Tables 10 and 11, it must be known that the image has been altered by digital zoom, and the resampling factor must be known so that the zoom can be reversed. One method studied analyzes statistical correlations to detect resampling factors[8]. However, there have been mixed results so far depending on the type of resampling used.

VI. COMPARISON TO PREVIOUS STUDIES

To compare our results to other methods of feature extraction and classification, we classified images using the higher order statistical features scheme[9]. This method was designed for detecting hidden messages in images, but can be extended to applications such as differentiation between brands of cameras. Tests were run using the original cell phone pictures and the cell phone pictures with additional JPEG compression. The results follow, using 90 images to train and 10 to test, 100 iterations, without using SFFS. As shown in Table 11, our features perform better in classification of original cell phone images and images with additional JPEG compression. Tests have not yet been performed on the scanner or standalone camera images using higher order statistical features.

Table 11. Comparison between classification of cell phone images using a combination of interpolation and noise features *without SFFS* and using higher order statistical features. The mean value for correct classification is given

Quality Factor	Interpolation/Noise	HOSF
100%	97.7%	85.6%
90%	94.4%	81.4%
80%	93.5%	77.4%
70%	91.8%	73%
60%	85.8%	68.8%

In previous work in [6] with identification of scanners using noise features and SVM classification, seven different models of scanners were tested using noise features only. In this case, there was a reported 95.6% success on average using the leave-one-out scenario. In our tests using four models of scanners, there was a 95.4% success rate on average using only noise features, but a 96.2% success rate on average using a combination of noise features and interpolation coefficients.

There are no known previous studies of classification by type of device.

VII. CONCLUSIONS

Non-intrusive component forensics aims as identifying the algorithms and parameters of a device solely based on its output data. Previous work on non-intrusive forensics have focused mainly on such imaging devices as digital cameras and scanners and, in this project, we extend these forensic techniques to cell phone cameras. The color interpolation coefficients and the noise feature parameters are estimated from the images and are jointly used as features for forensic analysis. We show that the combined set of features can provide tell-tale clues and accurately help trace the origin of the input image to its production process and help identify the cell phone camera brand and model that was used in its capture as well as to differentiate between camera-, scanner-, and computer-generated images. Detailed simulation results with 5 cell phone cameras, 5 scanners and 4 digital cameras suggest that the proposed techniques are very efficient giving an overall accuracy above 94%. Further, the proposed techniques are also robust to post-processing operations such as digital zoom and JPEG compression. We believe that such analysis can be extended to applications in identifying patent infringement and for tampering detection to help provide a common framework for digital image forensics.

REFERENCES

[1] A. Ferrari, “Camera Phones Fire A Warning Shot,” http://www.forbes.com/infoimaging/2003/12/10/cx_af_1210camera.html, Dec. 10 2003.

[2] Sources: InfoTrends/CAM Ventures; Lyra Research; www.clickz.com

[3] H. Gou, A. Swaminathan, and M. Wu, Intrinsic Sensor Noise Features for Forensic Analysis on Scanners and Scanned Images, to be submitted to *IEEE Transactions on Information Forensics and Security*, August 2007.

[4] Website www.almanazir.com last accessed on July 31 2007.

[5] A. Swaminathan, M. Wu, K.J. Ray Liu, “Component Forensics of Digital Cameras: A Non-Intrusive Approach,” *Proceedings of the international conference on information sciences and systems*, Princeton, NJ, Mar 2006.

[6] H. Gou, A. Swaminathan, and M. Wu, “Robust Scanner Identification based on Noise Features,” *Proceedings of the SPIE, Security, Steaganography and Watermarking of Multimedia contents,* San Jose, CA, January 2007.

[7] Website http://research.janelia.org/peng/proj/mRMR/index.htm last accessed on July 31 2007.

[8] Popescu and H. Farid, “Exposing Digital Forgeries by Detecting Traces of Resampling,” *IEEE Trans. on Signal Processing*, vol. 53, no. 2, part 2, pp. 758–767, Feb. 2005.

[9] S. Lyu and H. Farid, “Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines,” presented at the 5th Int. Workshop on Information Hiding, Noordwijkerhout, The Netherlands, 2002.

[10] M. Kharrazi, H. T. Sencar, and N. Memon, “Blind source camera identification,” Proc. of IEEE Intl. Conference on Image Processing, vol. 1, pp. 709–712, Singapore, Oct. 2004.

[11] 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. Conference on Digital Forensics, Orlando, FL, Jan. 2006.

[12] M-J. Tsai, C-L. Lai, and J. Liu, “Camera/Mobile Phone Source Identification for Digital Forensics”, Proc. of the IEEE international conference on Acoustic, Speech and Signal Processing, vol. 2, pp. 221—224, Honolulu, HI, April 2007.