THE IMPACT OF EXPOSURE SETTINGS IN DIGITAL IMAGE FORENSICS

Li Lin[⋆]*, Wenhao Chen*[⋆]*, Yangxiao Wang*[⋆]*, Stephanie Reinder*[⋆]*,*
Min Wu[†]*, Yong Guan*[⋆]*, and Jennifer Newman*[⋆]

[⋆] Iowa State University, Ames, IA, USA
[†]University of Maryland, College Park, MD, USA

ABSTRACT

The digital image forensics academic community is facing a growing challenge. The volume of images presented to digital image forensic practitioners increases every day, and with it, more variety of possible outcomes in image analysis. When an academic forensic tool is applied to a realistic case, the effects of imaging factors, including the noise level, should be seriously considered. Although there have been conjectures that shot noise would affect the empirical accuracy of a forensic analyzer, it has not yet received enough experimental support. In this paper, instead of estimating the noise, we inspect two measurable factors of exposure settings, ISO speed and exposure time, and present a set of experiments using mobile phone data to demonstrate the effect of exposure settings on steganalysis and PRNU-based camera device identification. Our results show that more investigations into the characteristics of image data with respect to exposure settings is required to fully understand identification or classification that is concerned with low-magnitude noise measurements, such as PRNU or stegoembedded messages.

Index Terms— Digital Image Forensics, Steganalysis, PRNU, Exposure Setting, ISO.

1. INTRODUCTION

With the advent of improved camera and editing apps on smartphones, the nature and authenticity of digital photos are becoming more questioned. This increasingly critical field, digital image forensics, is important to both the academic and forensic practitioner communities. Mobile devices, in particular, allow a user to easily send a message hidden in an image acquired on the device. Steganography changes intensity values of the image ever so slightly to represent the bit-valued message, with no visual indication in the scene. The process of detecting steganography using statistics, machine learning, and other means is called steganalysis. Another area of digital image forensics is camera identification. A digital image itself contains traces of the image-acquisition process that are represented in the observed intensity values of the photo, both from the imaging sensor and from the in-camera processing pipeline. For example, a sensor fingerprint such as the photo response non-uniformity (PRNU) can be extracted to identify the camera that acquired that photo [1].

For the purpose of development and benchmarking of image forensic procedures, several image datasets are offered by the academic community. These include BOSSbase [2], created for steganalysis, RAISE [3], created for image forgery and the Dresden Image Database [4], created for digital image forensics. Since the birth of these databases, the standards and principles of building an image database for image forensics have been discussed. For example, the diversity of cameras and scenes has an important factor since the beginning [5]. Although the impact of the noise levels in images has been shown to affect the performance of forensics [6, 7, 8], the impact of exposure settings, such as ISO speed and exposure time, which are highly correlated to image capture noise [9], has not yet been studied well. Some previous work, such as [10], reveals some unexpected phenomenon in the case study of camera identification with varied exposure times, but the work omitted testing the ISO settings. In [11], the authors took advantage of some extreme levels of ISO to design steganography embedding algorithms that are more secure, but it omitted the impact on exposure settings of original image data. Another recent work [12] claimed that the impact of ISO settings has minor impact on steganalysis for JPEG images, but it ignored the case for the spatial domain.

In this paper, we show the importance of exposure settings on two representative image forensics problems, namely, digital image steganalysis and camera identification. We first perform our experiments on the impact of ISO speed with image data from BOSSbase, and then analyze the effects of both ISO and exposure time on steganalyzing the image data collected by iPhones. In the case study of camera identification, we control all environmental variables to prominently reflect the main effects of ISO speed in identifying digital camera devices. As the first study on such a topic, our preliminary results also call attention to the roles of exposure noise levels in digital image forensics, especially for building a benchmarking image database.

The remainder of the paper is as follows: Section 2 pro-

Funded by NIST Center of Excellence in Forensic Science and Statistics.

vides some background information on camera exposure settings, digital steganography and steganalysis, and camera model and device identification. Section 3 discusses the experiments relating exposure settings to steganalysis and camera identification. We conclude in Section 4.

2. BACKGROUND KNOWLEDGE

Settings of Exposure in Digital Cameras. A digital camera captures photons and produces bits. ISO speed is a multiplicative gain to the voltage coming off the solid-state sensor, applied equally to scene signal and sensor noise. The exposure time measures, in seconds, the amount of time the aperture is open, allowing photons to be captured by the photo-sensitive material at each pixel. The intensity value in the final image is roughly proportional to the number of photons captured by an individual pixel, and includes effects of sensor noise and in-camera processing. In auto-exposure mode, a digital camera is programmed to choose an ISO value and exposure time, among other settings, which produces a digital photograph with a high signal-to-noise ratio (SNR) and low image noise. A lower ISO speed with appropriate exposure setting typically produces a photo with lower noise and higher signal (higher SNR), and better perceptual quality to a viewer [9]. One advantage of digital cameras over film cameras is that values for the cameras settings are saved as meta data in an EXIF file as part of the image data, and can be retrieved later to inspect the photo's exposure settings.

Digital Image Steganalysis is the analysis of image data to discover if hidden content is contained within the image, and, if so, to uncover further information about the hidden content. The vast majority of research has focused on identifying or classifying an image as cover (innocent) or stego (with hidden content). Machine learning (ML) algorithms have proven to be the workhorse of steganalysis. Classic ML requires feature extraction, a ML algorithm, and large amounts of data. After the HUGO competition [2] in 2010, the winners produced a new feature set and ML classifier, and these have been used as one of the top state-of-the-art for steganography and steganalysis benchmarking. The feature set is the Spatial Rich Model (SRM) [13], with 34,641 features, and the classifier is the ensemble classifier [14]. We implement the SRM with ensemble classifier for our ML algorithms, using code provided at Dr. Fridrich's website [15].

Camera Device Identification aims to identify an image as being acquired by one specific camera device. Typically, statistical tools are used to make the identification. In camera identification, PRNU has been well-studied and proven to be an effective method [1] [16]. PRNU is a sensor "fingerprint" that measures the differences in photon responses between individual pixel sites on the sensor and therefore it can be used to identify a specific device.

3. STUDY OF IMAGE FORENSICS WITH DIFFERENT EXPOSURE SETTINGS

3.1. Steganalysis under Different Exposure Settings

3.1.1. Experiments on BOSSbase

To study the impact of exposure settings on steganalysis, we begin with the data from BOSSbase, for it is the most frequently used database for benchmarking steganalysis. To reduce the impact from differences by camera models, we use only one camera to run the experiment on images with different exposure settings. After carefully analyzing the EXIF files, we select images taken by the PENTAX 20D in BOSSbase, as there are 603 images from this camera shot with ISO 200 and 358 images with ISO 100. To increase the sample size, we download the original raw images, convert to TIFF format by PhotoShop and then cut into five grey-scale images of dimension 512×512 without overlapping. This produces more than 1700 images with ISO 100 called Dataset 1, and 3000 images with ISO 200 called Dataset 2.

After constructing these two datasets, we implement the Spatial embedding algorithm "MiPOD" [17] with 0.1 payload size to both datasets. The SRM and ensemble classifier have been applied for feature extraction and classification, respectively. For each dataset, we randomly pick 800 images for training, and then test on 800 images chosen from the remaining images in the same dataset. We also test on another 800 images randomly chosen from the other dataset having the different ISO setting. The result of this experiment is provided in Table 1, and the error rate is computed as the average error of false alarms and missed detections.

As we can see from Table 1, applying a well-trained classifier to target data with different ISO brings significantly higher errors. For example, training on ISO 100 data and testing on ISO 100 data has error rate 20.15%, but if we apply this very classifier directly to test images with ISO 200, an unacceptable penalty with 46.33% error rate will be the consequence for ignoring the impact of ISO speed.

3.1.2. Experiments on Image Data from iPhones

Although BOSSbase contains images with a variety of ISO settings, many photos in BOSSbase were taken with auto exposure modes or half auto exposure modes. So this database is not suitable for studying the impact of exposure time on steganalysis. Additionally, different ISO settings with auto exposure modes usually imply a change in scene contents or

Table 1*: Error rates on different ISO data from BOSSbase.*

Test data ISO	Training data ISO	Avg. error rate
100	100	**20.15%**
	200	35.39%
200	100	46.33%
	200	**31.50%**

Table 2: *Misclassification rates on data with different exposure settings on iPhone 7. (In (a) and (b), exposure time is fixed as 1/200 s and 1/50 s respectively; in (c) and (d), ISO speed is fixed as 100 and 200 respectively.)*

Test data ISO	Training data ISO	Avg. error rate (a)	Avg. error rate (b)
100	100	**7.72%**	**14.92%**
	200	28.89%	24.93%
	1000	38.04%	40.70%
200	100	17.89%	26.18%
	200	**9.90%**	**18.67%**
	1000	30.39%	46.79%
1000	100	48.50%	42.16%
	200	42.18%	34.04%
	1000	**18.08%**	**12.57%**

Test exposure time	Training exposure time	Avg. error rate (c)	Avg. error rate (d)
1/200 s	1/200 s	**7.72%**	**9.90%**
	1/50 s	16.89%	20.52%
	1/10 s	37.88%	40.71%
1/50 s	1/200 s	24.47%	25.13%
	1/50 s	**14.92%**	**18.67%**
	1/10 s	27.89%	28.18%
1/10 s	1/200 s	34.31%	24.50 %
	1/50 s	24.09%	19.90 %
	1/10 s	**15.95%**	**12.20%**

light conditions when images are captured. To continue running experiments focusing on the main effects of exposure time, optimally we should collect images with various exposure settings on same scene content.

We choose the app "ProCam" [18] for our experiments on iPhones, since this app allows convenient selection of ISO and exposure time, and enables us to save the raw image in .dng or .tiff formats. With "ProCam" installed on three different iPhones from three models (6S, 6SPlus and 7), student photographers were tasked to collect large amounts of images. All photographers took a series of 10 images fixed on the same scene (all scenes were indoors at various locations), where the first photo was taken in auto exposure mode, and the remaining nine images were taken under specific settings with three ISO speeds: 100, 200, 1000 and three exposure times: 1/10 s, 1/50 s, and 1/200 s.

More than 1500 original tiff images were collected for each iPhone, producing 150 different scenes with the same exposure setting. To increase the sample size, we cut the original color images into five smaller grey images with dimension 512×512, as we did for BOSSbase. Therefore, for each phone, we now have 750 images as covers for each exposure setting, with 150 different scenes.

Spatial embedding algorithm MiPOD was implemented to all cover images with 0.1 payload size. We apply SRM for feature extraction and ensemble classifier for image classification as we did for BOSSbase data. For each phone, we randomly select 700 images with the same exposure setting for training and then test the trained classifier on 700 images with different exposure settings, repeating 10 times. That is, for each dataset with same exposure setting, 10-fold cross validation error was computed as a baseline to compare the performance with different classifiers. Most images with ISO 1000, exposure time 1/10 s are highly saturated, so we drop all results related to this setting. We observed that the results are quite similar across all three iPhones, so we only select results from experiments on iPhone 7 to present in Table 2.

In Table 2 (a) and (b), we fix the exposure time and compare the error rates for image datasets that have different ISO settings. The results from these two are similar to what we have learned from BOSSbase, that is, training the data with one ISO setting but testing the data with another ISO brings extra errors. In Table 2 (c) and (d), the ISO settings are both fixed. By changing the settings of exposure time, we discover that the exposure time also plays an important role as well as ISO speed. Take the detection classifier based on data with ISO 200, exposure time 1/10 for an example, the 12.20% error rate is low. However, if this classifier was used to test the data with the same ISO but shorter exposure time of 1/200, then there would be a 40.71% misdetection rate as penalty.

Based on results in Table 2 and all previous assumptions on methods and database, we conclude that, the lowest error rates happen when the training data and test data share the same exposure settings. Moreover, for the same test data, training on data with a larger difference in camera settings values bring higher error rates than relative closer settings. This observation leads us to the next experiment.

3.1.3. Discussions

According to the ISO standard [9], for every scene content, images with higher ISO or longer exposure time have larger grey values and more noise than images with lower ISO and shorter exposure time. Notice that scene content was fixed for experiments on iPhones, and images in BOSSbase are collected by half-auto or auto settings. We apply a wavelet denoiser [19] for all images we selected in BOSSbase to get a clean image, and then compute the noise as the mean variance for each individual image, given by

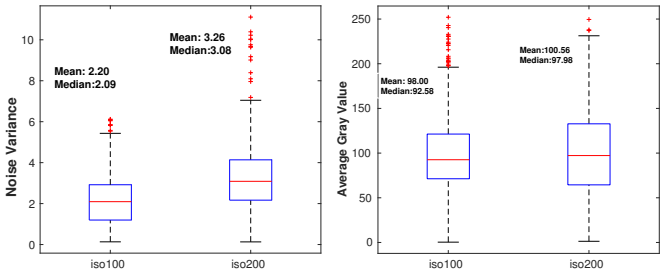
$$\sigma^2 = \frac{1}{m \cdot n} \sum_{i=1}^{m} \sum_{j=1}^{n} (F(i,j) - I(i,j))^2 \qquad (1)$$

where $F(i,j)$ is the grey value at coordinate (i,j), and $I(i,j)$ is the grey value after denoising. The results are provided as boxplot in Fig. 1.

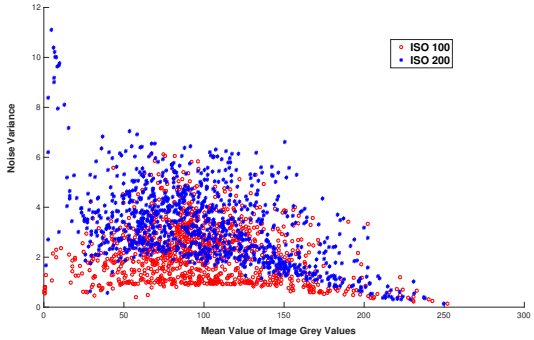
As we can see from Fig. 1 (a) and (b), there exists only a very slightly change in grey values for images with different ISO settings, while noise levels increase nearly 50% on average from ISO 100 to ISO 200. Fig. 1 (c) shows vividly that, on average, with the change in the mean grey values across all pixel values, noise associated with ISO 200 is higher than noise by ISO 100. Combining results from Fig. 1 with Table 1, it is very natural to associate the high error rate in the ISO-mismatch case, with the impact of noise variance. We are conducting further studies on this topic.

3.2. Camera Identification under Different ISO Settings

In this subsection,we design a simple experiment as an extreme case to analyze the effects of ISO settings in the de-



(a) Boxplots of Noise Levels (b) Boxplots of Grey Values



(c) Noise Levels v.s. Mean Grey Values

Fig. 1: *Plots of noise levels and average grey values for 2000 cover images from experiments on BOSSbase.*

vice identification problem. Two Google Pixel phones, labeled as Pixel-1 and Pixel-2 have been purchased. We start with two ISO settings, ISO 100 and ISO 1000, since ISO 100 is a typical setting for image outdoor images, and ISO 1000 is common for indoor images. In addition, we select a fixed exposure time of 1/50 s such that all photos collected in the experiments are neither too dark nor too bright. The device Pixel-1 is selected to generate its PRNU reference, and the other device, Pixel-2 is used for testing only. To simulate a scenario when the target device is not accessible, we did not use flat-field images, and instead collected 50 images taken with the exact same scene and same ISO 100 to produce the PRNU reference for Pixel-1. To reduce the impact of natural scene content when collecting these 50 images, we developed an app called "Cameraw" [20] for Android phones, which allows us to turn *off* the digital image stabilization and lock *all* camera settings during the photo collection. More importantly, it takes images with less than 0.5 seconds between each image acquisition. With "Cameraw" installed on the two Google Pixels, we implement the algorithm in [1] to generate the PRNU reference for Google Pixel-1 and a variety of other scene data for Pixel-1 and Pixel-2. The test database contains 200 images, 100 images from each device. For each device, 50 images are taken with the ISO 100 and 50 images are taken with ISO 1000. We compute the normalized correlation between the reference image and noise pattern extracted from

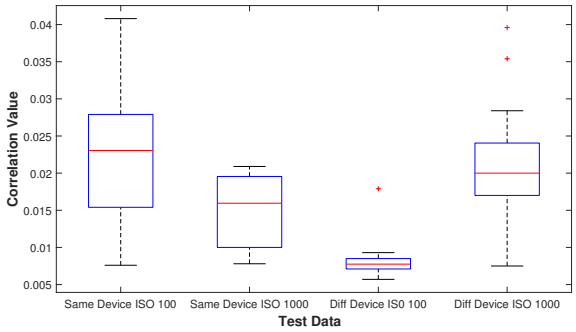


Fig. 2: *Normalized correlation values for noise patterns of two Google phones, where the PRNU reference is generated by 50 image with ISO 100 and exposure time 1/50 s from a fixed scene indoor.*

each test image. The correlation values are illustrated by boxplots in Fig. 2.

In Fig. 2, the lowest correlation values are between the ISO setting of 100 on different devices. However, it is surprising that test images from another device with high ISO 1000 have even greater correlation values, than images from the same device but taken by a different ISO setting. With such data, any advanced classifier based on PRNU correlations would fail to identify the correct device. This scenario could happen when the PRNU reference pattern is obtained from outdoor images, but the images to test are all shot inside of a building.

Our experiment on Google Pixel phones suggests that ISO also plays an important role in camera forensic analysis. Since the iOS version of Cameraw is still under development, we are not able to test for iPhones at this stage. However, the previous results call for the image forensics community to carry out more experimental studies and analysis in order to gain comprehensive understandings toward what ISO setting(s) should be used to compute a reference PRNU of a camera, and how reliable matching with a test image should be done for camera identification.

4. CONCLUSION AND FUTURE WORK

The primary goal of this paper is to explore the role of exposure settings in digital image forensics. The first two experiments reveal the effects of ISO speed and exposure time in steganalysis, and the third experiment shows the importance of ISO speed in camera identification problems. Our results show that, even for a fixed device, adapting the exposure parameters for the target images can significantly improve the performance of a forensic analyzer. In addition, to build an image database for benchmarking digital image forensics, the diversity of exposure settings for images in such a database must be taken into account. We plan to study the impact of exposure settings on other learning paradigms in future work.

5. REFERENCES

[1] J. Lukas, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, 2006.

[2] P. Bas, T. Filler, and T. Pevnỳ, "Break Our Steganographic System: The Ins and Outs of Organizing BOSS," in *Information Hiding*. Springer, 2011, pp. 59–70.

[3] D.-T. Dang-Nguyen, C. Pasquini, V. Conotter, and G. Boato, "RAISE: a raw images dataset for digital image forensics," in *Proceedings of the 6th ACM Multimedia Systems Conference*. ACM, 2015, pp. 219–224.

[4] T. Gloe and R. Böhme, "The 'Dresden Image Database' for Benchmarking Digital Image Forensics," in *Proceedings of the 2010 ACM Symposium on Applied Computing*, ser. SAC '10. New York, NY, USA: ACM, 2010, pp. 1584–1590.

[5] J. Fridrich, J. Kodovský, V. Holub, and M. Goljan, "Breaking HUGO – The Process Discovery," in *Information Hiding*, T. Filler, T. Pevný, S. Craver, and A. Ker, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 85–101.

[6] J. Fan, H. Cao, and A. C. Kot, "Estimating EXIF Parameters Based on Noise Features for Image Manipulation Detection," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 608–618, April 2013.

[7] V. Sedighi, J. Fridrich, and R. Cogranne, "Toss that BOSSbase, Alice!" *Electronic Imaging*, vol. 2016, no. 8, pp. 1–9, 2016.

[8] H. Gou, A. Swaminathan, and M. Wu, "Noise features for image tampering detection and steganalysis," in *Image Processing, 2007. ICIP 2007. IEEE International Conference on*, vol. 6. IEEE, 2007, pp. VI–97.

[9] International Standard Organization, "Photography – digital still cameras – determination of exposure index, iso speed ratings, standard output sensitivity, and recommended exposure index," ISO 12232:2006, 2006.

[10] T. Gloe, S. Pfennig, and M. Kirchner, "Unexpected artefacts in PRNU-based camera identification: a 'Dresden Image Database' case-study," in *Proceedings of the on Multimedia and security*. ACM, 2012, pp. 109–114.

[11] P. Bas, "Steganography via cover-source switching," in *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, Dec 2016, pp. 1–6.

[12] Q. Giboulot, R. Cogranne, and P. Bas, "Steganalysis into the wild: How to define a source?" *Electronic Imaging*, 2018.

[13] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 868–882, 2012.

[14] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432–444, 2012.

[15] "Steganography embedding (MiPOD) and feature extraction (SRM) software code," http://dde.binghamton.edu/download/.

[16] C.-T. Li, "Source camera identification using enhanced sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 280–287, 2010.

[17] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 221–234, 2016.

[18] S. Azzam, "ProCam," https://itunes.apple.com/us/app/procam-5/id730712409?mt=8.

[19] M. K. Mihcak, I. Kozintsev, and K. Ramchandran, "Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising," in *1999 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings. ICASSP99 (Cat. No.99CH36258)*, vol. 6, Mar 1999, pp. 3253–3256 vol.6.

[20] W. Chen, "Cameraw, an Android camera app for digital image forensics," CSAFE, Iowa State University, Tech. Rep., Oct. 2017.