The ‘Dresden Image Database’ for Benchmarking Digital Image Forensics

Thomas Gloe
Technische Universität Dresden
Institute of Systems Architecture
01062 Dresden, Germany
thomas.gloe@tu-dresden.de

Rainer Böhme
International Computer Science Institute
1947 Center Street, Suite 600
Berkeley, CA, 94704 USA
rainer.boehme@icsi.berkeley.edu

ABSTRACT

This paper introduces and documents a novel image database specifically built for the purpose of development and benchmarking of camera-based digital forensic techniques. More than 14,000 images of various indoor and outdoor scenes have been acquired under controlled and thus widely comparable conditions from altogether 73 digital cameras. The cameras were drawn from only 25 different models to ensure that device-specific and model-specific characteristics can be disentangled and studied separately, as validated with results in this paper. In addition, auxiliary images for the estimation of device-specific sensor noise pattern were collected for each camera. Another subset of images to study model-specific JPEG compression algorithms has been compiled for each model. The ‘Dresden Image Database’ will be made freely available for scientific purposes when this accompanying paper is presented. The database is intended to become a useful resource for researchers and forensic investigators. Using a standard database as a benchmark not only makes results more comparable and reproducible, but it is also more economical and avoids potential copyright and privacy issues that go along with self-sampled benchmark sets from public photo communities on the Internet.

Categories and Subject Descriptors

K.4.2 [**Social Issues**]: Abuse and Crime Involving Computers; I.4.7 [**Image Processing and Computer Vision**]: Feature Measurement; I.4.8 [**Image Processing and Computer Vision**]: Scene Analysis; I.4 [**Image Processing**]: Miscellaneous

General Terms

Algorithms, Security, Experimentation, Standardization

Keywords

Digital Image Forensics, Benchmarking, Image Source Identification, Camera Model Identification, Forgery Detection

SAC'10 March 22-26, 2010, Sierre, Switzerland.

1. MOTIVATION

Digital image forensics is a forensic science that analyses traces in image data to answer at least one of two questions: first, is a given digital image authentic or has it been altered? And second, is it possible to *link* digital images to their acquisition device or class of acquisition devices? Depending on the level of analysis, classes can be the device type (i. e., digital camera or scanner), the manufacturer, or model. In contrast to digital watermarking as authenticity technique, digital image forensics does not require any active embedding step at the time of creation or publication. Evidence is extracted merely from structural analysis of image files and statistical analysis of the image data (i. e., the two-dimensional array of pixel intensities).

There already exists an ample body of literature in the young but rapidly growing field of digital image forensics, e.g. [14, 9, 8, 11, 13]. However, experimental evidence in this literature is generally generated from custom-made data sets, which are not always made available to independent researchers, for various reasons. Consequently, the reproduction and validation of new techniques as well as the comparison between alternative techniques is a complicated and error-prone task. Note that this problem is not specific for digital image forensics. Large parts of the contemporary research in digital forensics is barely reproducible and representative corpora are needed to bring more scientific rigor to all sub-disciplines of (digital) forensics [4, 1].

The lack of a common benchmark data set in digital image forensics limits both comparability and reproducibility of results as well as the design of improved algorithms.[1] Comparability aside, it is also not economical for each team of researchers to do the fieldwork and compile their own data. To sum it up, we consider the existence of a common benchmark database as a sign of maturity of a field [15] and, in this contribution, introduce the ‘Dresden Image Database’ to fill this gap.

Great care has been taken to ensure that the database is most useful to researchers and forensic investigators alike. Our design goals were to build a comprehensive and extensible database of authentic digital photographs depicting realistic scenes. All images were acquired under controlled conditions, regarding all relevant influencing factors known for the current state of the art. The scenes have been carefully selected to avoid copyright violations and possible privacy

[1] A commendable exception is the image splicing database by [7]. However, it is limited to the detection of very basic attempts of manipulations. It includes only a small set of images and it does not control for scene content.

issues. For example, false positives or spurious correlation could falsely frame uninvolved individuals as suspects in a criminal investigation. For this reason forensic investigators in certain jurisdictions are not allowed to check a suspect image against a set of images acquired from uncontrolled sources, such as photo communities on the Internet. This limitation does not apply to our database, so it may be used as a reference for evidence to be used in court.

The remainder of this paper is organized as follows: Section 2 presents the design ideas and the procedure followed to acquire the set of benchmark images. Section 3 describes the contents and structure of the database and discusses details of auxiliary images to study device-specific sensor noise pattern and model-specific JPEG compression artifacts. The quality and usefulness of the database is demonstrated in Sec. 4 with exemplary results for camera model identification. Section 5 points to a web-based user interface for the database and Sec. 6 concludes the paper.

2. IMAGE ACQUISITION PROCEDURE

Developing and testing forensic methods for digital images requires a large body of images acquired under the following list of basic parameters: different imaged scenes, different acquisition devices, different device settings, and different environmental conditions. Depending on the scope of the forensic method under study, sound research tries to control for as many of these parameters as possible. In fact, the empirical nature of forensic sciences makes it indispensable to use comprehensive and valid data sets [2]. However, when we consider the number of possible parameter combinations, the effort increases dramatically.

Consider for example methods for camera model identification. They require a large number of images of different scenes made with a large number of different devices. However, to study the performance of camera model identification rigourously, more than one device is required per camera model. Moreover the influence of scene content and camera settings has to be considered. So images of each scene for each device and, in the ideal case, for different camera settings are needed. To the best of our knowledge, no image database fulfilling these requirements is freely available for research. And obviously, building such a comprehensive data set is a too time-consuming task to be repeated by each team of researchers.

The main purpose of the presented image database is to provide an extendable and reusable set of authentic images of the same scene for each digital camera in our test setup covering different camera settings as a basis for developing and benchmarking image forensic methods.[2] Recall that a large number of images with very similar scene content is the key to study device-dependent, model-dependent and manufacturer-dependent characteristics in detail. So we selected 25 camera *models* spanning all relevant *manufacturers* and price ranges (i. e., very simple cameras with fixed lens up to semi-professional digital SLR cameras) and collected up to 5 *devices* for each model. In most cases more than one model was available for each manufacturer. This enables to study the similarity of characteristics between models of the same manufacturer as well as between manufacturers.

[2]In case of forgery detection algorithms, additional faked images are required. The proposed database can be a starting point to create such manipulated images [10], though manipulated images are not part of the database, yet.

Figure 1: Examples of indoor and outdoor scenes—natural and man-made—in the 'Dresden Image Database'. (The bottom-left image shows all cameras of set A on the desktop.)

For logistic reasons, the altogether 73 cameras were divided into two *image sets* (A and B) while ensuring that all devices of the same model always belong to the same set. Landscape and portrait images were acquired at various *positions* around the picturesque city of Dresden in wintertime (to escape the crowds of tourists). Typical examples for acquired scenes are depicted in Fig. 1.

The general image acquisition procedure is illustrated in Fig. 2. At each position, up to two *motives* were fixed with tripods, and three or more *scenes* have been taken from each motive. Different scenes for one motive differ by their focal length (by default, minimum and maximum focal lengths as well as one comparable setting between models has been acquired). For each scene, at least one *image* exists with default settings (full automatic or, if applicable, programme mode), and a second image was taken with deactivated flash in case the camera automatic has flashed in the default setting. The assignment of each image to its scene, motive and position is given with respective identifiers in the database so that images can be selected and compared across settings, manufacturers, models and devices within the image set.

Most consumer cameras by default store images in lossy compressed JPEG format. To minimize the impact of such post-processing inside the camera, we configured all cameras to the highest available JPEG quality setting and maximum available resolution. When supported by the camera, additional losslessly compressed images were stored.

3. CONTENT AND ORGANISATION

Table 1 shows the list of selected camera models and their corresponding number of available devices. It includes also basic information on the model specifications and statistics of the flash launches. Overall, the database contains enough images to draw subsets with constant flash setting or focal lengths to quantitatively study the sensitivity of forensic techniques to these properties. It also allows to study the stability of lens aberrations in natural scenes. Therefore, the convertible lenses of the two Nikon D200 SLR digital

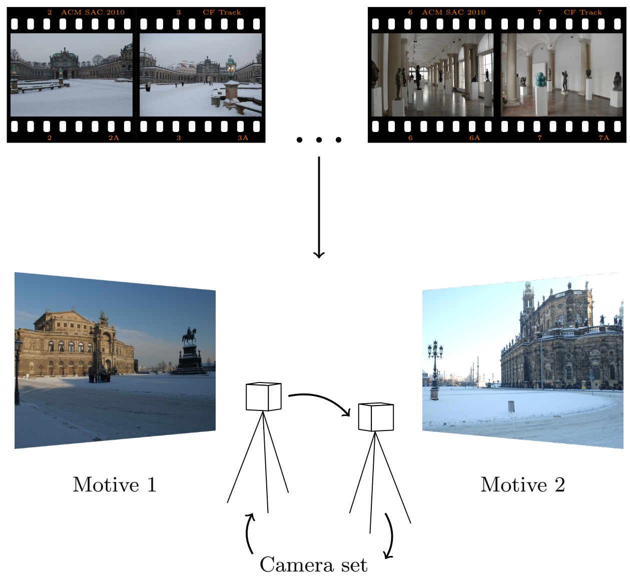

Figure 2: Acquisition procedure: at each position, up to two motives were fixed with tripods, and photographed with each camera of one set with systematically varying camera settings (flash, focal length and interchanging lens, if possible).

cameras were interchanged between both devices for each acquired scene. Additionally, two identical lenses were used for the Nikon D70/D70s SLR digital cameras. These lenses were interchanged for each acquired image between two (out of four) camera bodies.

To study the device-specific sensor noise pattern of all cameras in the image database, 50 *dark frame* images and 50 *flatfield* images were acquired for each device. The lens was covered to acquire the dark frames and a homogeneously backlit screen was used to acquire the flatfield frames. These auxiliary images are ready to analyse the stable parts of the sensor noise pattern separately: fixed pattern noise (FPU) and photo-response non-uniformity (PRNU). This allows, among others, research on ways to suppress or to forge the device-specific sensor noise pattern (cf. [12, 6]).

Another subset of images was created to specifically study model-specific JPEG compression algorithms. Some digital cameras apply JPEG compression independently from scene content (i. e., fixed quality), whereas others adaptively adjust their JPEG quantisation tables to the complexity of the scene content (i. e., fixed target file size). To study this interaction and compile a database of plausible JPEG quantisation tables per model, two scenes were designed to analyse model-specific JPEG compression algorithms as a function of the scene content. Figure 3 depicts the two JPEG-scenes, one scene with homogenous areas and low complexity, and one with pronounced colour contrast and higher complexity. Both scenes were acquired with one device of each model, thereby iterating over all combinations of possible image sizes, image quality settings, and flash enabled or disabled.

All images in the database are stored with and are referenced by an unique identifier, a cryptographic hash value (SHA1) to ensure the image integrity. The images are linked to the applied parameter values during image acquisition,

Figure 3: The two special scenes specifically designed to study the model-specific JPEG compression algorithm.

like the corresponding scene of an image, the camera model or the applied camera settings. Further, manually coded tags describing the visual quality in terms of visible image defects, image distortions (out of focus, camera blur) are available per image. This enables the selection of subsets (possibly excluding technically 'bad' images) by specifying parameter values of interest. Figure 4 summarises the basic structure of the database with a simplified entity relationship model. Entities are represented by rectangles, relations are represented by diamonds and attributes are represented by circles. The cardinality of functional relations between entities are indicated by 1 or N. So for each position, two tripods were fixed to capture scenes of two motives. Every motive is further characterised by the scene type (e. g., urban, natural or auxiliary) and the environment, i. e., indoor or outdoor. For each motive, N images were acquired using different devices and different camera settings for focal length, flash and the employed lens. Each device corresponds to one model and one manufacturer. Note that for brevity, not all available attributes are printed in Fig. 4.

Besides the image acquisition parameters, the image database is also designed to store measured *features* for each image. For example, such features can be used to determine the manufacturer, model or device of the acquisition device from the image alone. There are two main advantages of storing the calculated features. First, if one re-implements other researchers' methods as starting point for own experiments, stored features along with the underlying images can be a valuable reference to eliminate ambiguities (and spot errors). Second, in certain cases the time-consuming re-implementation and feature extraction of alternative analysis methods can be completely avoided while still being able to compare their performance to newly developed methods. Both puts researchers in a better position to provide sound evaluation results with reasonable effort (cf. [4]).

4. EVALUATION

In this section we present a first practical evaluation of the image database. One way to assess the quality of an image database is the absence of saturation due to over- or underexposure. This is so because saturated areas in images hide model and device-specific characteristics and distort typical forensic algorithms. Figure 5 shows a histogram of the fraction of saturated pixels in image set A: all images have been converted to 8-bit greyscale and pixels count as saturated if their value is either below 5 or above 250. These thresholds were chosen to reflect a typical level of noise in consumer digital cameras. In both image sets, 97% of all images con-

Table 1: Digital camera models included in the 'Dresden Image Database': number of devices per model, basic camera specifications and number of available images.

Camera Model	No. Devices	Resolution [Pixel]	Sensor Size [inch or mm]	Focal Length [mm]	No. Images Set A (flash off/on)	No. Images Set B (flash off/on)
AgfaPhoto DC-504	1	4032×3024	-	7.1	84 (70/14)	80 (70/10)
AgfaPhoto DC-733s	1	3072×2304	-	6.2−18.6	151 (130/21)	166 (163/3)
AgfaPhoto DC-830i	1	3264×2448	-	6.2−18.6	183 (132/51)	217 (183/34)
AgfaPhoto Sensor 505-X	1	2592×1944	-	7.5	87 (76/11)	104 (95/9)
AgfaPhoto Sensor 530s	1	4032×3024	-	6.1−18.3	199 (149/50)	198 (160/38)
Canon Ixus 55	1	2592×1944	1/2.5"	5.8−17.4	186 (143/43)	-
Canon Ixus 70	3	3072×2304	1/2.5"	5.8−17.4	542 (428/114)	-
Casio EX-Z150	5	3264×2448	1/2.5"	4.65−18.6	925 (748/177)	-
Fujifilm FinePix J50	3	3264×2448	1/2.5"	6.2−31.0	-	495 (433/62)
Kodak M1063	5	3664×2748	1/2.33"	5.7−17.1	999 (692/307)	1161 (920/241)
Nikon Coolpix S710	5	4352×3264	1/1.72"	6.0−21.6	916 (743/173)	-
Nikon D70/D70s	2/2	3008×2000	23.7×15.6 mm	18−200	715 (637/78)	-
Nikon D200 Lens A/B	2	3872×2592	23.6×15.8 mm	18 − 135/17 − 55	712 (633/79)	-
Olympus μ1050SW	5	3648×2736	1/2.33"	6.7−20.1	1027 (686/341)	-
Panasonsic DMC-FZ50	3	3648×2736	1/1.8"	7.4−88.8	-	561 (493/68)
Pentax Optio A40	4	4000×3000	1/1.7"	7.9−23.7	-	629 (540/89)
Pentax Optio W60	1	3648×2736	1/2.3"	5.0−25.0	-	146 (129/17)
Praktica DCZ 5.9	5	2560×1920	1/2.5"	5.4−16.2	973 (706/267)	-
Ricoh Capilo GX100	5	3648×2736	1/1.75"	5.1−15.3	-	715 (632/83)
Rollei RCP-7325XS	3	3072×2304	1/2.5"	5.8−17.4	581 (433/148)	-
Samsung L74wide	3	3072×2304	1/2.5"	4.7−16.7	562 (425/137)	-
Samsung NV15	3	3648×2736	1/1.8"	7.3−21.9	566 (456/110)	-
Sony DSC-H50	2	3456×2592	1/2.3"	5.2−78.0	-	308 (284/24)
Sony DSC-T77	4	3648×2736	1/2.3"	6.18−24.7	-	565 (506/59)
Sony DSC-W170	2	3648×2736	1/2.3"	5.0−25.0	-	272 (246/26)
$\sum$	73				9408 (7287/2121)	5617 (4854/763)

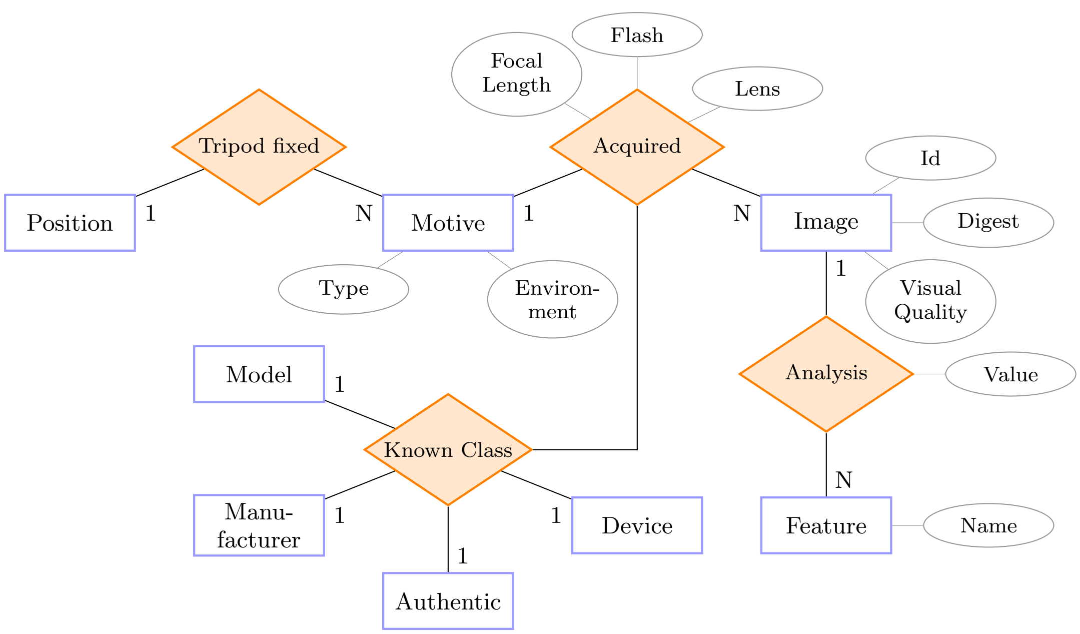

Figure 4: Simplified entity relationship model of the 'Dresden Image Database'

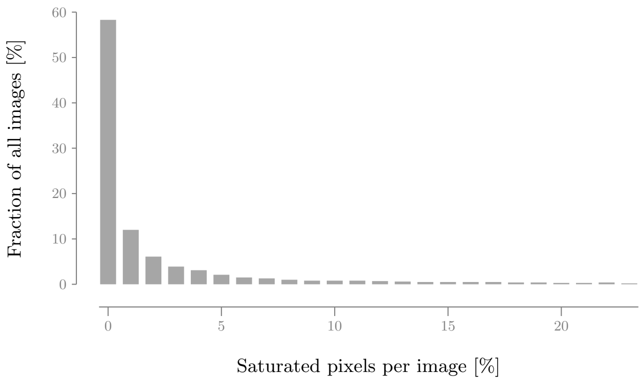

Figure 5: Histogram of saturation due to over- or underexposure in the image database. The plot covers 97% of all images, whereas the negligible amount of remaining images contain more than 24% of saturated pixels.

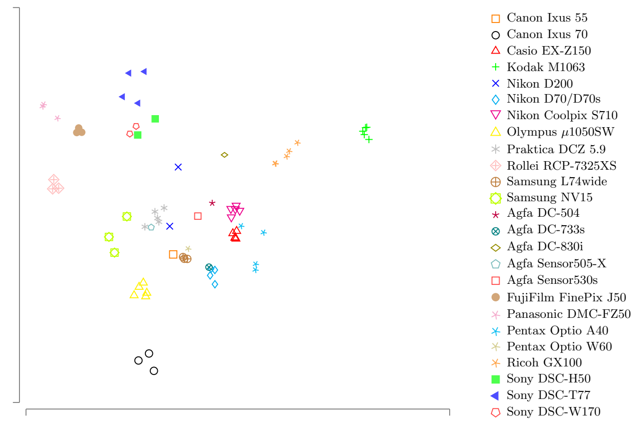

Figure 6: Visualisation of intra-model similarity and inter-model dissimilarity. Multi-dimensional scaling of device centroids in a reduced feature space, annotated with model labels. The feature space has been reduced to the ten most influential features using a PCA-based feature sensitivity measure.

tain less than 25% saturated pixels. In 90% of the images, the number of saturated pixels per image is less than 10%. A differentiation between saturation in bright and dark areas shows that in 96% of the images, the number of saturated pixels in bright areas is less than 10%; and in 95% of the images, the number of saturated pixels in dark areas is less than 10%.

To practically evaluate the suitability of our database for the development and evaluation of image forensic methods, we ran feature-based camera model identification, as proposed by Kharrazi, Sencar and Memon [9], on the image database. As the name suggests, feature-based camera model identification is based on analysing 34 different features which capture the characteristics of the different camera components of a digital camera (e. g., image quality, image noise, image sharpness or colour reproduction). Additionally, our extended feature set was included in the practical evaluation [5].

Based on the calculated features for all images, Fig. 6 exemplary depicts the distance in feature space between all devices in the image database, annotated with the model names. The plot is generated by reducing the feature-space to the 10 most influential features using a sensitivity measure based on the principal component analysis. The result clearly demonstrates the dissimilarity between models, whereas the calculated features for devices of the same model are closer to each other. Compared to previous work including only 5 or 12 different camera models [9, 5], the results reported here document that feature-based camera model identification is also practical in large-scale scenarios.

Furthermore, the calculated features were used to train a machine learning algorithm[3] to identify the employed camera model automatically. Therefore, 60% of the images of one device per model were selected to train the machine learning algorithm, and all images of the remaining devices were used for testing. This procedure was iterated over all devices per model. Table 2 summarises the test results. Note, only models with more than one device were selected for this test scenario. As documented in Tab. 2, the overall true positive rate is approximately 96%. The detailed identification results vary between different camera models, from assigning all images correctly (Nikon Coolpix S710, Ricoh GX100) to correct identification rates around 90% for the Sony DSC-T77 and the Pentax Optio A40.

The discrimination problems between models Nikon D70 and Nikon D70s were investigated by training both camera models separately. As the differences between camera models D70 and D70s are negligible due to a minor version update, the correct assignment of images made with these camera models is worse compared to all other results. However, the majority of all images made with the D70/D70s camera models are assigned to one of both models. This emphasises experimentally the expected similarity between Nikon D70 and Nikon D70s.

Both, the calculated image histograms as well as the calculated features will be made available in the image database.

[3]We employed the support vector machine libSVM with a radial based kernel function to separate different camera models [3].

5. USER INTERFACE

The ‘Dresden Image Database’ will be made freely available to other researchers for scientific purposes and can be accessed under the following URL: `http://forensics.inf.tu-dresden.de/dresden_image_database/`. The website enables browsing and downloading the provided images. For each image the associated meta informations—like image histograms, camera EXIF information, quantisation tables, and image features—are available through the website.

The web interface to the image database enables to create subsets of images according to the specified needs of a researcher, i. e., selecting images by categories like manufacturer, model, device, visual quality or camera settings. Beyond a simple ‘image gallery’, the web interface also provides functions to share the created image subsets between users and to support discussions of single images, image subsets or known classes of images. Users are invited to comment images and, by this, to share and strengthen their knowledge.

Table 2: Identification results using 60% of the images of one device per model for training (96.42% TPR)

Camera model		Identified as																		
		S	DT	DS	DSs	DC	FZ	H	T	W	E	F	G	I	L	M	N	O	R	μ
Coolpix S710	S	**100.00**	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
D200	DT	-	**93.73**	-	-	-	0.52	0.10	-	0.05	2.77	-	-	2.61	-	-	-	0.05	-	0.16
D70	DS	-	-	**84.57**	15.43	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
D70s	DSs	-	0.11	**67.51**	30.90	-	-	-	-	-	0.85	-	-	0.63	-	-	-	-	-	-
DCZ 5.9	DC	-	-	0.72	0.64	**98.42**	-	-	-	-	0.12	-	-	-	-	-	-	-	-	0.10
DMC-FZ50	FZ	-	1.14	-	-	-	**97.31**	0.50	0.58	0.32	-	0.06	-	-	-	-	0.09	-	-	-
DSC-H50	H	-	-	-	-	-	0.20	**98.23**	0.20	1.28	-	-	0.10	-	-	-	-	-	-	-
DSC-T77	T	-	0.74	-	-	-	3.43	2.04	**91.90**	1.81	-	-	0.09	-	-	-	-	-	-	-
DSC-W170	W	-	0.65	-	-	-	-	0.52	0.26	**98.06**	-	-	0.52	-	-	-	-	-	-	-
EX-Z150	E	-	-	0.19	0.08	-	-	-	-	-	**99.71**	-	-	-	0.03	-	-	-	-	-
FinePixJ50	F	-	-	-	-	-	0.06	-	-	-	-	**99.94**	-	-	-	-	-	-	-	-
GX100	G	-	-	-	-	-	-	-	-	-	-	-	**100.00**	-	-	-	-	-	-	-
Ixus70	I	-	-	0.79	0.47	-	-	-	-	-	-	-	-	**98.26**	0.42	-	-	-	-	0.05
L74wide	L	-	-	0.04	0.04	-	-	-	-	-	-	-	-	1.25	**98.66**	-	-	-	-	-
M1063	M	0.07	0.67	-	0.01	-	0.01	-	-	-	0.04	-	-	0.01	-	**99.19**	-	-	-	-
NV15	N	0.47	0.47	-	-	-	4.07	-	-	0.05	-	-	-	0.05	-	-	**92.85**	0.09	-	1.96
OptioA40	O	3.97	0.13	0.09	-	-	0.17	-	0.13	-	0.52	-	0.22	0.17	-	0.09	2.28	**90.86**	-	1.38
RCP-7325XS	R	-	-	-	-	0.21	-	-	-	-	-	-	-	-	-	-	-	-	**99.79**	-
μ1050SW	μ	-	0.29	-	-	-	0.12	-	-	-	-	-	-	0.14	0.10	-	0.38	0.02	-	**98.95**

Within future releases of the image database, a function to upload new feature descriptions and new feature values will be also made available.

6. CONCLUDING REMARKS

Recently, Garfinkel et al. (in line with the U. S. National Acadamy of Sciences) emphasized the need for publicly available and well-documented forensic reference data sets to make forensic results reproducible and comparable [4, 1]. Considering the limited time and financial resources of research groups and the need for reference data sets in education [4], the 'Dresden Image Database' is designed to fill the current gap for digital image forensics by providing a useful resource for investigating camera-based image forensic methods.

Overall more than 14,000 images covering different camera settings, environments and specific scenes facilitate rigorous analyses of manufacturer-, model- or device-dependent characteristics and their relation to other influencing factors. Furthermore, the image database is expected to enable independent researchers to verify their results on a publicly available dataset.

Contrary to the use of images collected from photo communities, our database provides authentic digital images together with well-documented parameters, like the photographed scene and the used camera settings. Furthermore, the 'Dresden Image Database' avoids copyright or privacy issues. The maintainer will ensure the long-term availability of the image data set and extend the database by including special sets of auxiliary images for the measurement of lens aberrations, and by including self-made fake images in the near future. The possibility to upload and share computed features into the 'Dresden Image Database' is deemed an accelerator for development and accuracy of new image forensic methods. The modular design of the 'Dresden Image Database' also enables to integrate new image data sets within future releases.

Acknowledgements

The authors gratefully acknowledge the staff members of the faculty of computer science, the staff members of the AVMZ (TU Dresden), and the following companies (in alphabetical order) for borrowing digital cameras: AgfaPhoto & Plawa, Casio, FujiFilm, Kodak, Nikon, Olympus, Pentax, Praktica, Ricoh, Rollei, Samsung and Sony. Special thanks go to the administration of Palaces and Gardens Dresden and to the administration of the Sculpture Collection Dresden for granting photography permissions for some very beautiful positions. We are indebted to all colleagues and friends supporting the creation of the underlying image database actively during some of the probably coldest days of the year 2009.

7. REFERENCES

[1] *Strengthening Forensic Science in the United States – A Path Forward.* The National Academies Press, Washington, D.C., 2009.

[2] R. Böhme, F. Freiling, T. Gloe, and M. Kirchner. Multimedia forensics is not computer forensics. In Z. J. M. H. Geradts, K. Y. Franke, and C. J. Veenman, editors, *Computational Forensics, Third International Workshop, IWCF 2009, The Hague, The Netherlands, August 13-14, 2009, Proceedings*, *LNCS* 5718, pages 90–103, Berlin, Heidelberg, 2009. Springer-Verlag.

[3] C.-C. Chang and C.-J. Lin. *LIBSVM: A library for support vector machines.* Software available at `http://www.csie.ntu.edu.tw/~cjlin/libsvm`, 2001.

[4] S. Garfinkel, P. Farrell, V. Roussev, and G. Dinolt. Bringing science to digital forensics with standardized forensic corpora. *Digital Investigation*, 6:S2–S11, 2009.

[5] T. Gloe, K. Borowka, and A. Winkler. Feature-based camera model identification works in practice – results of a comprehensive evaluation study. In *11th Information Hiding, Darmstadt, Germany, June 8-10, 2009, Revised Selected Papers*, *LNCS* 5806, pages 262–276, Berlin, Heidelberg, 2009. Springer-Verlag.

[6] T. Gloe, M. Kirchner, A. Winkler, and R. Böhme. Can we trust digital image forensics? In *MULTIMEDIA '07: Proceedings of the 15th international conference on Multimedia, September 24–29, 2007, Augsburg, Germany*, pages 78–86, New York, NY, USA, 2007. ACM Press.

[7] Y.-F. Hsu and S.-F. Chang. Detecting image splicing using geometry invariants and camera characteristics consistency. In *Proceedings of the 2006 IEEE International Conference on Multimedia and EXPO (ICME 2006)*, pages 549–552, 2006.

[8] M. K. Johnson and H. Farid. Exposing digital forgeries by detecting inconsistencies in lighting. In

MM&Sec'05, Proceedings of the Multimedia and Security Workshop 2005, August 1-2, 2005, New York, NY, USA, pages 1–10, 2005.

[9] M. Kharrazi, H. T. Sencar, and N. Memon. Blind source camera identification. In *Proceedings of the 2004 IEEE International Conference on Image Processing (ICIP 2004)*, pages 709–712, 2004.

[10] M. Kirchner and T. Gloe. On resampling detection in re-compressed images. In *First IEEE International Workshop on Information Forensics and Security (WIFS '09)*, 2009.

[11] J. Lukáš, J. Fridrich, and M. Goljan. Determining digital image origin using sensor imperfections. In A. Said and J. G. Apostolopoulus, editors, *Proceedings of SPIE: Image and Video Communications and Processing*, volume 5685, pages 249–260, 2005.

[12] J. Lukáš, J. Fridrich, and M. Goljan. Digital camera identification from sensor noise. *IEEE Transactions on Information Forensics and Security*, 1(2):205–214, 2006.

[13] T.-T. Ng, S.-F. Chang, C.-Y. Lin, and Q. Sun. Passive-blind image forensics. In W. Zeng, H. Yu, and C.-Y. Lin, editors, *Multimedia Security Technologies for Digital Rights*, chapter 15, pages 383–412. Academic Press, 2006.

[14] A. C. Popescu and H. Farid. Statistical tools for digital forensics. In J. Fridrich, editor, *Information Hiding. 6th International Workshop, IH 2004, Toronto, Canada, May 2004, Revised Selected Papers*, *LNCS* 3200, pages 128–147, Berlin, Heidelberg, 2004. Springer Verlag.

[15] H. T. Sencar and N. Memon. *Overview of State-of-the-art in Digital Image Forensics*. Statistical Science and Interdisciplinary Research. World Scientific Press, 2008.