Live System Forensics for Internet Videos

Ajay Gadicha #1, Dr. M.V.Sarode *2

[1] *P.R.Patil College of Engineering and Technology, Amravati, Maharastra, India*
ajjugadicha@gmail.com
[2] Jagdambha College of Engineering and technology Yavatmal, *Maharastra, India*

Abstract— The increasing transmission of illegal videos over the Internet imposes the needs to develop large-scale digital video forensics systems for prosecuting and deterring digital crimes in the Internet. In this paper, we propose, design, and implement a novel large-scale Digital Forensics Service Platform (*DFSP*) that can effectively detect illegal content from Internet videos. More specifically, we propose a distributed architecture by taking advantage of Content Delivery Network (CDN) to improve scalability, which can process enormous number of Internet videos in real time. We propose CDN-based Resource-Aware Scheduling (CRAS) algorithm, which schedules the tasks efficiently in the *DFSP* according to resource parameters, such as delay and computation load. We deploy the *DFSP* system in the Internet, which integrates the CDN-based distributed architecture and CRAS algorithm with a large-scale video detection algorithm, and evaluate the deployed system. Our evaluation results demonstrate the effectiveness of the platform.

Keywords— *Content delivery network, digital forensics, load balancing, Resource scheduling, video detection*

1. Introduction

There are fewer reported works on the efficiency and scalability for large-scale video content identification, which mainly focus on solving these problems from video retrieval algorithm perspective. This paper aims to address the efficiency and scalability issues from system perspective. There are two key challenges on large-scale forensics system for Internet videos:

- The large amount of computation brought by analysing and detecting large volume of video data. This makes it difficult to serve a large number of users concurrently.
- The large amount of communication brought by transmitting a great volume of video data from media sources to the system. To address the above challenges, in this paper we propose, design, and implement a novel large-scale Digital Forensics Service Platform (*DFSP*) to effectively and efficiently detect illegal contents from large-scale Internet videos.To solve the scalability problem, we propose to build *DFSP* upon CDN [7]. Existing CDN-based distributed architectures to improve the performance of media applications include Video-on-Demand (VoD) systems [8]–[11], live video streaming systems [12]–[14], collaborative media streaming systems [15]–[17], etc. *DFSP*, by using CDN, can push the massive forensics tasks to the most appropriate *CDN nodes*, thereby effectively reducing the computational cost and the communication cost.

To solve the efficiency problem, we propose CDN-based Resource-Aware Scheduling (CRAS) algorithm. Existing network- aware resource scheduling algorithms include non-adaptive scheduling algorithms that use some heuristics to select nodes [18]–[20], and adaptive scheduling algorithms that take the current network or server conditions into account [21]–[23].In *DFSP*, with CRAS algorithm, user requests can be directed to appropriate nodes. Different forensics tasks are assigned to different CDN nodes based on not only the network conditions but also the computation load, thereby the massive data stream can be in parallel scheduled among multiple nodes efficiently. Moreover, in the work, we propose to integrate the proposed CDN-based distributed architecture and CRAS algorithm with a Large-scale Video Detection (LVD) algorithm. To summarize, the main contributions of this paper are as follows: • We propose and design a novel large-scale digital video forensics service architecture and platform, which can process enormous number of Internet videos in real time by employing CDN. We propose a CDN-based Resource-Aware Scheduling algorithm for dynamic load balancing in *DFSP*, which can significantly improve the efficiency of the platform.• We implement and evaluate a deployed system in large scale, which integrates the CDN-based distributed architecture and the CDN-based resource-aware scheduling algorithm with a large-scale video detection algorithm.

2. Related Works

In this section we overview the related works on digital video forensics techniques and digital video forensics systems.

2.1 Digital Video Forensics Techniques

In the past few years, there has been a rapid growth on research in digital video forensics.

Watermarking is a traditional forensics technique for detecting illegal copies and digital tampering [24]–[26]. It has three aspects for improvement: 1) the watermark must be embedded in legal videos prior to video distribution; 2) the nature of the original data will be changed; and 3) the watermark could be attacked or destroyed during transmission. Other than watermarking, there exists a class of statistical techniques for detecting digital tampering [27]–[29]. Recently, video fingerprint technique has drawn wide attention [30]–[32]. Different from other forensics techniques, this technique can identify illegal content by extracting a unique fingerprint from video data. The fingerprint can be extracted based on some static features such as color [33], texture [34] and shape [35], or some motion features of the video [36], [37]. The major advantage of fingerprint technique is that the fingerprint can be extracted after the media has been distributed and will not change the original data; thus, it is a very useful method for detecting Internet videos.

2.2 Digital Video Forensics Systems

With the development of digital video forensics techniques, some forensics systems have been studied and implemented. Douze et al. presented a video copy detection system [1], which used a precise representation method to decide whether or not query video segment was a copy of a video from the indexed dataset. Xu et al. explored an effective system for analysing the high-level structures and extracting useful features from soccer videos in order to identify the content of videos [2]. Gauch and Shivadas presented a commercial identification system by extracting features from video sequences that can characterize the temporal and chromatic variations within each clip [3]. Shen et al. outlined a system for detecting near-duplicate videos based on the dominating content and content changing trends of the videos [4]. In addition to the above systems, some other similar ones also provided effective methods for video forensics and achieved good results. However, all this work analyses and processes videos on a single server.

To improve the forensic efficiency, some researchers began to study the data structure for effectively indexing the video features. However, the approaches are all based on single server. For example, Hoad and Zobel used local alignment to find sequences of similar values in video and clip, which provided much faster searching [38]. Lejsek et al. achieved good efficiency greatly depending on a specific hardware configuration, which is outside the range of usual computer workstations [39]–[41]; thus, their work may not be practical for large-scale deployments. Zhao et al. improved the scalability of several well-known features including color signature and visual keywords for web-based retrieval by using high-dimensional indexing techniques [5]. Recently, Shang *et al.* introduced a compact spatiotemporal feature to represent videos and constructed an efficient data structure to address the efficiency and scalability issues for real-time large-scale near-duplicate Web video retrieval [6]. Although these works have made good use of the server capacity, when the number of videos continues to scale up, the real-time performance may be still hard to be guaranteed.

3. System Architecture

Fig. 1 depicts the *DFSP* system architecture. It consists of three main components: Content Access (CA), Video Detection (VD), and Resource Management (RM), explained below: 1) Content Access (CA): It is located on each CDN node, which is used to obtain video data from certain media sources. During this process, we use web crawler [42], a special technology for web search, to collect data. This technology can methodically scan or “crawl” through Internet pages to create an index of video data, so that CA can quickly provide the relevant data to detect and regularly ensure the data are up to date. 2) Video Detection (VD): VD is a group of servers distributed near CDN nodes, which are responsible for analyzing video content and judging their legality. It is composed of “Blacklist” Database, Content Analysis Servers, and Searching and Matching Servers. “Blacklist” Database stores a copy of fingerprints of improper videos. Content Analysis Servers are used to analyze the video content and extract their fingerprints. Searching and Matching Servers take charge of comparing these fingerprints with those pre-stored in “Blacklist” Database, and judging their legality. We propose a large-scale video detection algorithm in VD, which will be presented in detail in Section IV.3) Resource Management (RM): RM controls and monitors the whole platform, in charge of scheduling, coordinating, and managing all the resources and tasks. It comprises Network Monitoring module and Load Balancing module. Since each node has a copy of “blacklist”, the forensics tasks can be done at any node. Network monitoring module is in charge of monitoring all the nodes and media sources, so that Load Balancing module can coordinate each node and schedule different tasks depending on the overall situation. To balance the load among multiple nodes, we propose CDN-based Resource-Aware Scheduling algorithm, which will be discussed in Section V in detail.

DFSP working flow is as follows. When a user requests to detect a media source (e.g., http://www.youku.com/), the request is first transferred to RM. RM takes into account of the location of the designated media source and the current load of each node to find an appropriate node for the media source. The user request is then redirected to the selected node. CA of the selected node obtains video data from the designated media source, caches them, and transfers them to VD. After that, VD of the selected node analyzes the video content coming from the designated media source and extracts their fingerprints. These fingerprints are compared with those pre-stored in “Blacklist” Database.

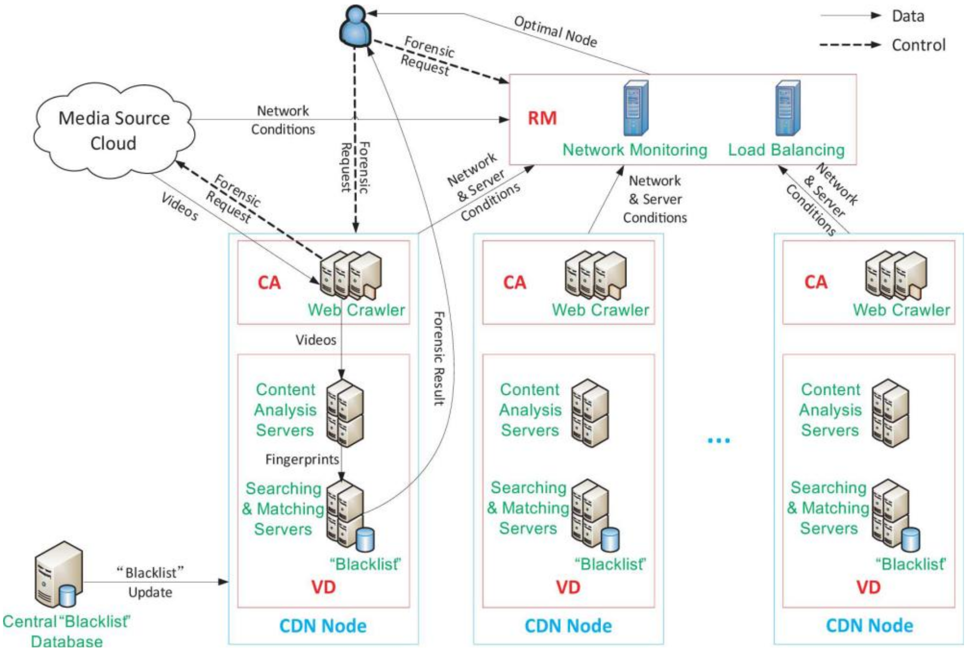

Fig.1: Block diagram

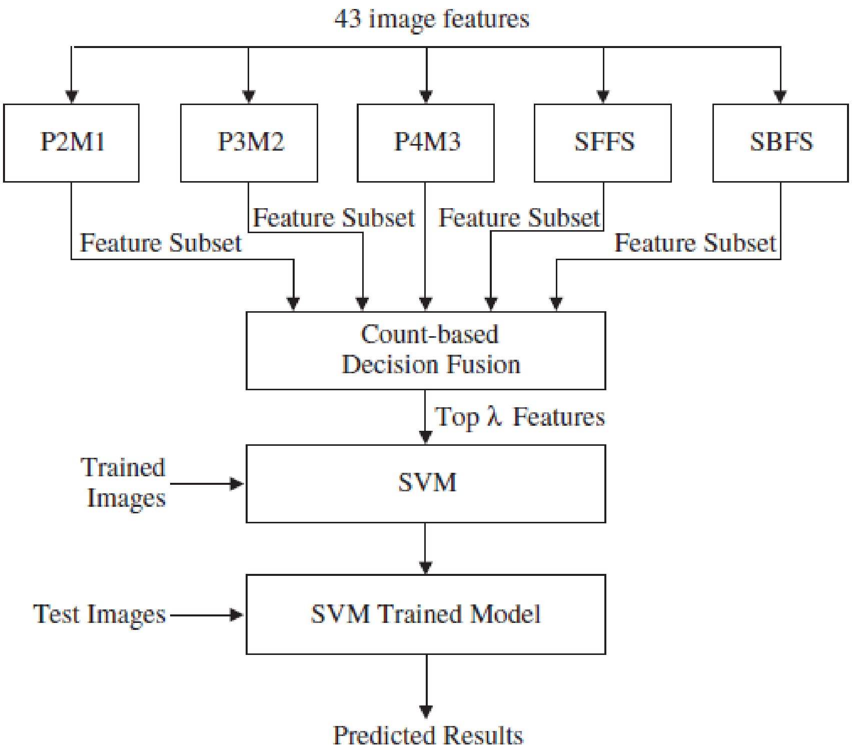

Fig. 2: Flow Chart

Finally, the legality of these videos, which is determined by the comparison result, is returned to the user.

4. Image Forensic

Image analysis is used in image forensic to expose the information using the image support machine with decision fusion techniques [4]. The author proposes a model that identifies the source model or device of an image by using the support vector machine approach along with decision fusion techniques. The paper considers feature selection algorithms as features in optimal subsets are generated in a series of inclusion and exclusion steps and count based aggregation as the algorithm of decision fusion. The algorithm selects the top λ features from 43 features in order to get the highest identification rate and the SVM trained model is built where test images is fed into the trained model to predict the camera source model.

As the imaging analysis being enhanced, contributes reviewing the state-of-the-art image registration methods that lays the foundations on evolutionary computation and analyzes the 3D modeling of forensic objects. The paper includes different evolutionary approaches in order to represent the wide variety of techniques within the EC paradigm and an IR method based on the classical ICP algorithm proposed by Liu. The paper reveals that the majority of the EIR methods following a parameter-based approach achieve the best and the most robust performance and the poor performance obtained by the matching- based methods.

With the highly advanced application, the forensic tool is able to differentiate between the fake and real image. By using multi resolution decomposition and higher order local autocorrelations *(HLACs*) image features are extracted and determine if it is real or fake [12]. They are used and as by right of the inner product lemma of higher order autocorrelation, the feature extraction and SVM are joined and the computation complexity is decreased significantly. The paper suggests Two dimensional discrete wavelet transformation (2D-DWT), a powerful multi resolution analysis tool. The signal characteristics in detail can be localized in different position, orientation and scale and multi resolution decomposition contains many intrinsic characteristics of natural images and fake images.

As Noise degradation causes failure to blind forgery detection methods, in [9] the author proposes a model that divides a suspected image into different partitions with homogenous noise levels. However, the authentic images also can contain various isolated regions with very different variations, which make the proposed method a supplement to other forgery detection methods rather than a standalone forgery detector. The proposed method is not able to find the corrupted regions, when the noise degradation is very small ($\sigma < 2$). The proposed method can be achieved by omitting the blocks merging step.

5. Memory forensics

Examines the information captured from memory at the time the computer is seized. As less focus has been paid to extracting information from Windows drivers, developing a methodology to minimize the effort of analyzing these drivers.

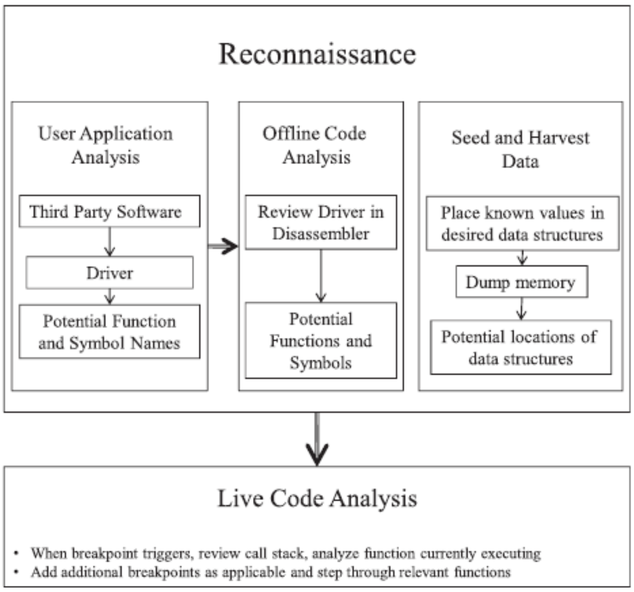
Reconnaissance
User Application Analysis
Third Party Software
Driver
Potential Function and Symbol Names
Offline Code Analysis
Review Driver in Disassembler
Potential Functions and Symbols
Seed and Harvest Data
Place known values in desired data structures
Dump memory
Potential locations of data structures
Live Code Analysis
• When breakpoint triggers, review call stack, analyze function currently executing
• Add additional breakpoints as applicable and step through relevant functions

Fig.3: Diagrammatic representation for code analysis

6. Forensic Tools for Video Acquisition Analysis

The analysis of image acquisition is one of the earliest problems that emerged in multimedia forensics, being very similar to the “classical” forensic technique of ballistic fingerprinting. Its basic goal is to understand the very first steps of the history of content, namely identifying the originating device. The source identification problem has been approached from several standpoints. We may be interested in understanding: (i) which *kind* of device/technique generated the content (e.g. camera, scanner, photo realistic computer graphics, etc.), (ii) which model of a device was used or, more specifically, (iii) which device generated the content. Different techniques address each of these problems in image forensics, and some of them have naturally laid the basis for the corresponding video forensic approaches.

7. Video coding parameter identification

In image and video coding architectures, the choice of the coding parameters is driven by non-normative tools, which depend on the specific implementation of the codec and on the characteristics of the coded signal. In JPEG

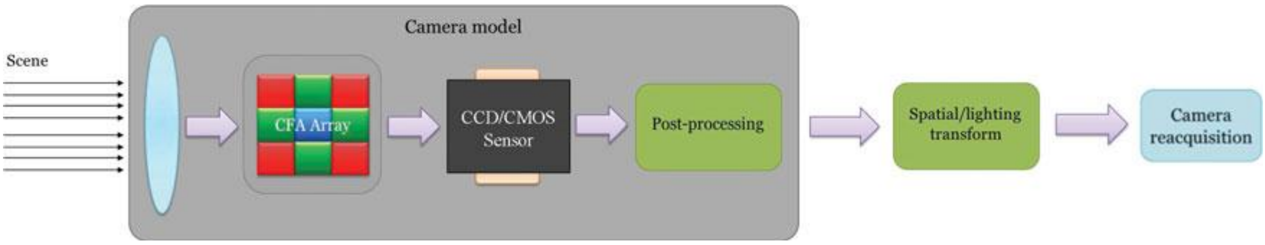

Fig.4: Camera reacquisition modelling

compression, the user-defined coding parameters are limited to the selection of the quantization matrices, which are adopted to improve the coding efficiency based on the psycho-visual analysis of human perception. Conversely, in the case of video compression, the number of coding parameters that can be adjusted is significantly wider. As a consequence, the forensic analyst needs to take into account a larger number of degrees of freedom when detecting the codec identity. This piece of information might enable the identification of vendor-dependent implementations of video codec's. As such, it could be potentially used to: (i) verify intellectual property infringements; (ii) identify the codec that generated the video content; (iii) estimate the quality of the reconstructed video without the availability of the original source. In the literature, the methods aiming at estimating different coding parameters and syntax elements characterizing the adopted codec can be grouped into three main categories, which are further described below: (i) approaches detecting block boundaries; (ii) approaches estimating the quantization parameters, and (iii) approaches estimating the motion

8. Video compression anti-forensics

An anti-forensic approach for JPEG compression has been recently proposed in [63]. There, the traces of compression are hidden by adding a dithering noise signal. Dithering is devised to reshape the histogram of DCT coefficients in such a way that the original Laplacian distribution is restored. In a following work by the same authors [64], a similar strategy is proposed to erase the traces of tampering from an image and hide double JPEG compression. This is achieved by a combined strategy, i.e., removing blocking artifacts by means of median filtering and restoring the original distribution of DCT coefficients with the same method as in [63]. In this way, the forensic analyst is not able to identify the tampered region by inspecting the distribution of DCT coefficients. However, it has been recently shown that anti-forensic methods are prone to leave their own footprints. In, the authors study the distortion which is inevitably introduced by the anti-forensic method in and propose an effective algorithm to counter it.

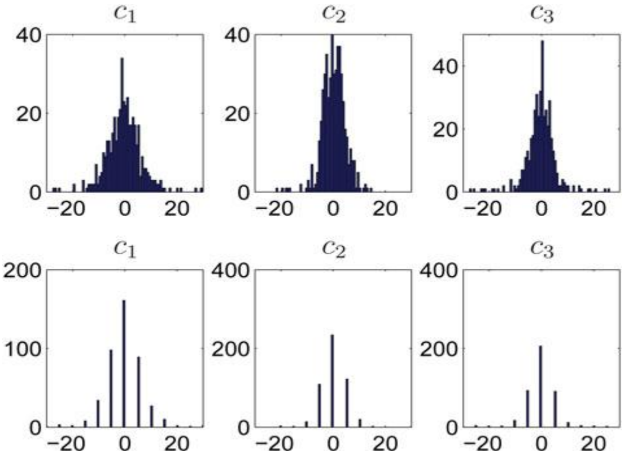

Fig.4: Histogram of DCT coefficients

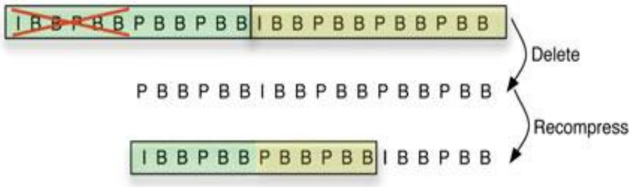
I B B P B B P B B P B B I B B P B B P B B P B B
Delete
P B B P B B I B B P B B P B B P B B
Recompress
I B B P B B P B B P B B I B B P B B

Fig. 5: Result

9. Conclusions and Future Works

As it has been shown in the previous sections, video forensics is nowadays a hot research issue in the signal processing world opening new problems and investigation threads. Despite several techniques have been mutated from image forensics, video signals pose new challenges in the forensic application world because of the amount and the complexity of data to be processed and the wide employment of compression techniques, which may alter or erase footprints left by previous signal modifications. This paper presented an overview of the state-of-the-art in video forensic techniques, underlying the future trends in this research field. More precisely, it is possible to divide video forensic techniques into three macro-areas concerning the acquisition, the compression, and the editing of the video signals.

References

[1] Farid, H.: Exposing digital forgeries in scientific images, in Proc. 8th Workshop on Multimedia and Security (MM&Sec 2006), September26–27, 2006, 29–36.

[2] Venkatraman, D.; Makur, A.: A compressive sensing approach to object-based surveillance video coding, in Proc. of IEEE Int. Conf. On Acoustics, Speech and Signal Processing (ICASSP 2009), Taipei, Taiwan, April 19–24, 2009, 3513–3516.

[3] Wang, W.; Farid, H.: Detecting re-projected video, in Information Hiding, Lecture Notes in Computer Science, K. Solanki, K. Sullivan, and U. Madhow, eds., vol. 5284, Springer, Berlin 2008, 72–86. 16 s. milani ET AL.

[4] Wang, W.; Farid, H.: Exposing digital forgeries in video by detecting double MPEG compression, in MM&Sec, S. Voloshynovskiy, J. Dittmann, and J. J. Fridrich, eds., ACM, 2006, 37–47.

[5] Sencar, H.T.;Memon, N.:Overview of State-of-the-art in Digital Image Forensics, Part of Indian Statistical Institute Platinum Jubilee Monograph series titled 'Statistical Science and Interdisciplinary Research' World Scientific Press, 2008.

[6] Poisel, R.; Tjoa, S.: Forensics investigations of multimedia data: a review of the state-of-the-art, in 2011 Sixth Int. Conf. on IT Security Incident Management and IT Forensics (IMF), Stuttgart, Germany, May 10–12, 2011, 48–61.

[7] Fridrich, J.: Image watermarking for tamper detection, in ICIP (2), 1998, 404–408.

[8] Eggers, J.; Girod, B.: Blind watermarking applied to image authentication, in 2001 IEEE Int. Conf. on Acoustics, Speech, and Signal Processing, 2001. Proc. (ICASSP '01), vol. 3, 2001, 1977–1980.

[9] Venkatesan, R.; Koon, S.-M.; Jakubowski, M. H.; Moulin, P.: Robust image hashing, in ICIP, 2000.

[10] Roy, S.; Sun, Q.: Robust hash for detecting and localizing image tampering, in ICIP (6). IEEE, 2007, 117–120.

[11] Tagliasacchi, M.; Valenzise, G.; Tubaro, S.: Hash-based identification of sparse image tampering. IEEE Trans. Image Process, 18(11) (2009), 2491–2504.

[12] Cossalter, M.; Tagliasacchi, M.; Valenzise, G.: Privacy-enabled object tracking in video sequences using compressive sensing, in Proc. of IEEE Int. Conf. on Advanced Video and Signal Based Surveillance (AVSS 2009), Genova, Italy, Sept. 2009, 436–441.

[13] Lin, Y.-C.; Varodayan, D. P.; Girod, B. Image authentication using distributed source coding. IEEE Trans. Image Process., 21(1) (2012), 273–283.

[14] Valenzise, G.; Tagliasacchi, M.; Tubaro, S.; Cancelli, G.; Barni, M.: A compressive-sensing based watermarking scheme for sparse image tampering identification, in Proc. 16th IEEE Int. Conf. on Image Processing (ICIP 2009), IEEE, Cairo, Egypt, November 7–10, 2009, 1265–1268.

[15] Lukas, J.; Fridrich, J.; Goljan, M.: Digital camera identification from sensor pattern noise. IEEE Trans. Info. Forensics and Secur., 1(2) (2006), 205–214.

[16] Chen, M.; Fridrich, J. J.; Goljan, M.; Lukas, J.: Determining image origin and integrity using sensor noise, IEEE Trans. on Info. Forensics Secur., 3(1) (2008), 74–90.

[17] Popescu, A.; Farid, H.: Exposing digital forgeries in color filter array interpolated images, IEEE Trans. Signal Process., 53(10) (2005) 3948– 3959.

[18] Johnson, M. K.; Farid, H.: Exposing digital forgeries through chromatic aberration, in MM&Sec, S. Voloshynovskiy, J. Dittmann, and J. J. Fridrich, eds., ACM, 2006, 48–55.

[19] Yerushalmy, I.; Hel-Or, H.: Digital image forgery detection based on lens and sensor aberration, Int. J. Comput. Vis., 92(1) (2011), 71–91.

[20] Milani, S.; Tagliasacchi,M.; Tubaro,M.: Discriminatingmultiple jpeg compression using first digit features, in Proc. of the 37th Int.Conf. on Acoustics, Speech, and Signal Processing (ICASSP 2012), March 25–30, 2012, 2253–2256.

[21] Fu, D.; Shi, Y. Q.; Su,W.: A generalized benfords law for jpeg coefficients and its applications in image forensics, in Proc. of SPIE, Security, Steganography and Watermarking of Multimedia Contents IX, vol. 6505, January 28–February 1, 2009, 39–48.

[22] Liu, H.;Heynderickx, I.:Ano-reference perceptual blockinessmetric, in ICASSP, IEEE, 2008, 865–868.

[23] Lin, W. S.; Tjoa, S. K.; Zhao, H. V.; Liu, K. J. R.: Digital image source coder forensics via intrinsic fingerprints, IEEE Trans. Info. Forensics Secur., 4(3) (2009), 460–475.

[24] Fan, Z.; de Queiroz, R. L.: Maximum likelihood estimation of JPEG quantization table in the identification of bitmap compression history,
in ICIP, 2000.

[25] Fan, Z.; de Queiroz, R. L.: Identification of bitmap compression history: JPEG detection and quantizer estimation, IEEE Trans. Image Process., 12(2) (2003), 230–235.

[26] Lukas, J.; Fridrich, J.: Estimation of primary quantization matrix in double compressed jpeg images, in Proc. of DFRWS, 2003.

[27] Lin, Z. C.; He, J. F.; Tang, X.; Tang, C. K.: Fast, automatic and finegrained tampered JPEG image detection viaDCT coefficient analysis, Pattern Recognit., 42(11) (2009) 2492–2501.

[28] Bianchi, T.; Piva, A.:Detection of non-aligned double JPEG compression with estimation of primary compression parameters, in 2011 18th IEEEInt.Conf. on ImageProcessing (ICIP), September 2011, 1929–1932.

[29] Bianchi, T.; De Rosa, A.; Piva, A.: Improved DCT coefficient analysis for forgery localization in JPEG images, in ICASSP, IEEE, 2011, 2444–2447.

[30] Bianchi, T.; Piva, A.: Detection of nonaligned double jpeg compression based on integer periodicity maps, IEEE Trans. Info. Forensics Secur., 7(2) (2012), 842–848.

[31] Johnson, M. K.; Farid, H.: Exposing digital forgeries in complex lighting environments, IEEE Trans. Info. Forensics Secur., 2(3–1) (2007), 450–461.

[32] Johnson, M. K.; Farid, H.: Exposing digital forgeries through specular highlights on the eye, in Information Hiding, Lecture Notes in Computer Science, T. Furon, F. Cayre, G. J. Doerr, andP.Bas, eds., vol. 4567, Springer, 2007, 311–325.

[33] Zhang, W.; Cao, X.; Zhang, J.; Zhu, J.; Wang, P.: Detecting photographic composites using shadows, in ICME, IEEE, 2009, 1042–1045.

[34] Conotter, V.; Boato, G.; Farid, H.: Detecting photo manipulation on signs and billboards, in ICIP, IEEE, 2010, 1741–1744.

[35] Kurosawa, K.; Kuroki, K.; Saitoh, N.: Ccd fingerprint methodidentification of a video camera fromvideotaped images, in Proc. 1999 Int. Conf. on Image Processing, 1999. ICIP 99., vol. 3, 1999, 537–540.

[36] Holst, G. C.: CCD Arrays, Cameras, and Displays, 2nd edn. CD Publishing & SPIE Press, 1998.

[37] Amerini, I.; Caldelli, R.; Cappellini, V.; Picchioni, F.; Piva, A.: Analysis of denoising filters for photo response non uniformity noise extraction in source camera identification, in 2009 16th Int. Conf. on Digital Signal Processing, July 2009, 1–7.

[38] Chen, M.; Fridrich, J.; Goljan, M.; Lukas, J.: Source digital camcorder identification using sensor photo response non-uniformity, in Proc. SPIE, 2007.

[39] Kivanc Mihcak, M.; Kozintsev, I.; Ramchandran, K.: Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising, in Proc., 1999 IEEE Int. Conf. on Acoustics, Speech, and Signal Processing,, vol. 6, March 1999, 3253–3256.

[40] Van Houten,W.;Geradts, Z. J.M.H.; Franke, K.;Veenman, C. J.:Verification of video source camera competition (camcom2010), in ICPR Contests, Lecture Notes in Computer Science, D. Unay, Z. Cataltepe, and S. Aksoy, eds., vol. 6388. Springer, 2010, 22–28.

[41] Van Houten, W.; Geradts, Z. J. M. H.: Using sensor noise to identify low resolution compressed videos from youtube, in IWCF, Lecture Notes in Computer Science, Z. J. M. H. Geradts, K. Franke, and C. J. Veenman, eds., vol. 5718. Springer, 2009, 104–11 vectors.