Flicker Forensics for Pirate Devices Identification

Adi Hajj-Ahmad
University of Maryland
College Park, USA

Séverine Baudry
Technicolor R&D France
Cesson-Sévigné, France

Bertrand Chupeau
Technicolor R&D France
Cesson-Sévigné, France

Gwenaël Doërr
Technicolor R&D France
Cesson-Sévigné, France

ABSTRACT

Cryptography-based content protection is an efficient means to protect multimedia content during transport. Nevertheless, content is eventually decrypted at rendering time, leaving it vulnerable to piracy e.g. using a camcorder to record movies displayed on an LCD screen. Such type of piracy naturally imprints a visible flicker signal in the pirate video due to the interplay between the rendering and acquisition devices. The parameters of such flicker are inherently tied to the characteristics of the pirate devices such as the back-light of the LCD screen and the read-out time of the camcorder. In this article, we introduce a forensic methodology to estimate such parameters by analyzing the flicker signal present in pirate recordings. Experimental results clearly showcase that the accuracy of these estimation techniques offers efficient means to tell-tale which devices have been used for piracy thanks to the variety of factory settings used by consumer electronics manufacturers.

Categories and Subject Descriptors

[**Hardware**]: Input/Output and Data Communications—*Input/Output Devices*; [**Computing Methodologies**]: Image Processing and Computer Vision—*Digitization and Image Capture, General*; [**Computing Milieux**]: Computers and Society—*Public Policy Issues*

General Terms

Security, Algorithm.

Keywords

Passive forensics, piracy, LCD screen, back-light, camcorder, rolling shutter, read-out time, flicker.

IH&MMSec'15 June 17-19, 2015 Portland, OR, USA
 ISBN 978-1-4503-3587-4/15/06 ...$15.00
DOI: http://dx.doi.org/10.1145/2756601.2756612.

Figure 1: Flicker artifact when recording an LCD screen displaying a uniformly gray frame with a camcorder.

1. INTRODUCTION

Movie piracy still remains a major concern for the Entertainment industry today. Disclosure on unauthorized sharing platforms prior to theatrical/Blu-ray releases holds the potential to significantly harm revenues. To address this risk, content owners routinely rely on cryptography-based content protection techniques to prevent consumers from easily accessing multimedia content [15]. Nevertheless, such protection has to be lifted eventually to render the content and a pirate then only has to place a camera in front of the screen to record a pirate copy of the movie.

A second line of defense then consists of embedding forensic watermarks within the rendered content, which can survive digital-analog-digital conversion [4]. As a result, when a pirate copy surfaces on unauthorized distribution platforms, it is possible to recover the underlying watermark identifier and trace it back to the user or device from which the piracy originated [7]. Such a traitor tracing mechanism has already been deployed in digital cinemas [5] and is anticipated to be soon extended to the consumer's home to protect ultra high definition content [12].

In this context, it is worth studying the piracy path when pirate video samples are obtained by camcording an LCD screen. As depicted in Figure 1, such a piracy scenario is known to yield a visible flicker signal due to the interplay between the camcorder and the screen. It is incarnated by typical dark/bright stripes that scroll up/down the pirate video. In prior work, research efforts have been dedicated

to detect the presence of such flicker [13, 14, 11, 3]. Indeed, this tell-tale artifact provides clues about the piracy path and can be exploited by the forensic analyst to select which watermark detector to use. More recently, notable efforts have been spent to reverse the flicker distortion [16, 1] in order to improve watermark detection performances for instance.

In this paper, we intend to investigate whether the characteristics of the flicker signal present in a pirate copy could be exploited to infer which devices have been used to produce it. For instance, relying on some traitor-tracing evidence, police investigators may have raided the home of a suspect pirate and seized a collection of devices. It would therefore be useful to provide corroborating evidence that the flicker signal observed in the pirate movies could be produced using these devices. Moreover, in case watermark-based tracing mechanisms fail, it could provide a fall-back mechanism to link pirate samples together which originate from the same piracy workflow.

In Section 2, we start by reminding how the flicker signal is formed prior to deriving a mathematical identity that connects the read-out time of the camcorder and the back-light frequency of the LCD screen to some characteristics of the flicker signal, namely its vertical radial frequency. We detail two alternate methods in Section 3 to illustrate how this characteristic value can be estimated directly from the frames of a camcorded video sequence. We then review three forensic scenarios in Section 4 and detail how to identify the pirate devices in each case. Such analysis usually requires having access to the ground-truth parameters of the suspect devices and we therefore briefly describe a methodology to extract them in Section 5. Experimental results reported in Section 6 clearly indicate that the flicker signal present in camcorded movies is indeed useful to pinpoint which devices have been used in the piracy workflow. In Section 7, we summarize our findings, discuss the limitations of the proposed approach and outline directions for future work.

2. CONNECTING THE FLICKER SIGNAL TO THE PIRATE DEVICES

When placing a camcorder in front of an LCD screen, the interaction between the back-light of the screen and the acquisition mechanism of the camcorder is known to yield visible flicker in the video recording.

The image appearing on an LCD screen is formed by the light that is let through by an array of liquid crystal cells, each cell encoding a pixel of the image [2]. Each individual liquid crystal can be tuned by changing the electric potential applied to it in order to let more or less light pass. In other words, a key feature of an LCD display design is the presence of a source of light to illuminate the array of liquid crystal cells from behind. This so-called *back-light* is a periodical signal whose frequency is high enough to be imperceptible by the human eye, typically around 200 Hz.

On the other hand, camcorders have an array of built-in sensors which is exposed to light for a given period of time. The resulting electrical charge accumulated by each sensor is then converted to produce the pixel values of the video frame. With camcorders routinely operating between 24 and 60 frames per second (fps), several cycles of the back-light will be integrated during the acquisition period. Since the back-light of the screen and the shutter of the camcorder are not synchronized, different frames of the video recording are associated to different sections of the back-light signal. As a result, the average luminance varies periodically at a frequency given by the aliasing of the high-frequency back-light signal by the low-frequency acquisition process.

Moreover, most camcorders commercially sold nowadays use CMOS sensors and a *rolling shutter* [8, 9]. In contrast with global shutters that acquire a whole frame at once, a rolling shutter captures each line sequentially e.g. from top to bottom. Consequently, each row of the image sees a different portion of the back-light and the average luminance of the recorded video now also varies along the vertical direction as exemplified in Figure 1. According to prior work [1], such spatio-temporal flicker can be modeled as follows:

$$\mathbf{f}[x, y, t] = (A \cdot \mathbf{c}[x, y, t] + B) \cdot \cos(\omega_t \cdot t + \omega_y \cdot y + \phi), \quad (1)$$

where x, y and t are respectively the column, row, and time indices and $\mathbf{c}$ is the luminance of the displayed video content. The first term of the equation indicates that the amplitude of the flicker scales linearly with the luminance of the camcorded content as given by the linear coefficients A and B. The second term captures the periodical nature of the flicker signal both in time and along the rows. The temporal radial frequency ω_t is given in radians/frame and the vertical radial frequency ω_y is given in radians/row. The phase ϕ accommodates for the absence of synchronization between the back-light and the shutter.

As mentioned earlier, a camcorder typically captures video frames at a rate f_c that is much smaller than the fundamental frequency f_BL of the back-light. In other words, the camcorder operates below the Nyquist rate and the flicker signal therefore ends up at an aliased frequency f_t of the back-light, i.e.

$$\exists k \in \mathbb{N}, \quad f_t = |f_\mathrm{BL} - k \cdot f_\mathrm{c}| < \frac{f_\mathrm{c}}{2}. \quad (2)$$

The temporal radial frequency is then given by $\omega_t = 2\pi f_t / f_\mathrm{c}$. In contrast, the read-out time T_ro taken by a camcorder to capture a video frame usually ranges between 10-35 ms. As a result, the vertical sampling rate is on the order of 10 kHz, i.e. much larger than the Nyquist sampling rate of a regular back-light signal. There is thus no aliasing and the vertical radial frequency can be written as:

$$\omega_y = 2\pi \cdot \frac{f_\mathrm{BL}}{f_y}, \quad (3)$$

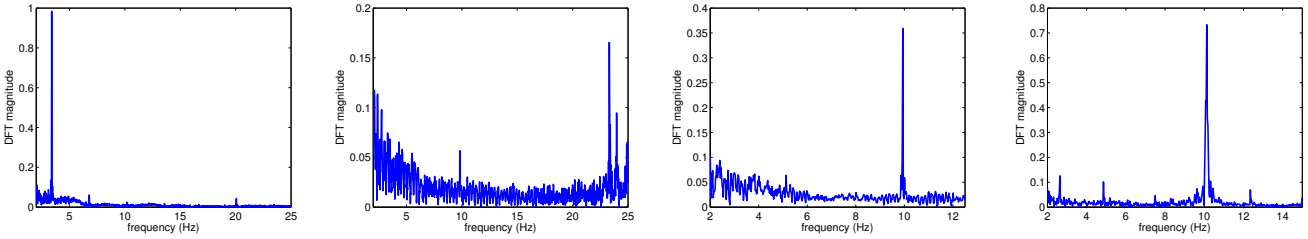
where $f_y = H/T_\mathrm{ro}$ can be seen as the row acquisition rate if H denotes the number of rows in a video frame. It is then straightforward to establish the following mathematical identity:

$$T_\mathrm{ro} \cdot f_\mathrm{BL} = \frac{H \cdot \omega_y}{2\pi}, \quad (4)$$

that links some characteristics of the pirate devices, namely the read-out time T_ro of the camcorder and the back-light frequency f_BL of the LCD screen, together with some property of the flicker signal present in the video signal.

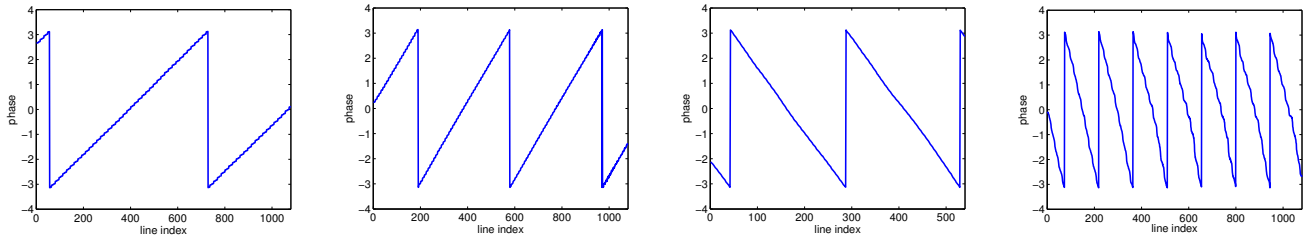
3. ESTIMATION OF THE VERTICAL RADIAL FREQUENCY

A straightforward investigation strategy consists of extracting the characteristic quantities appearing in the right-hand side of Equation (4) from the pirate sample and then



(a) $f_t \approx 3.39$ Hz (b) $f_t \approx 23.3$ Hz (c) $f_t \approx 9.94$ Hz (d) $f_t \approx 10.13$ Hz

Figure 2: Magnitude of the Fourier transform of one row average $\mathbf{r}[y^*, t]$ for several pirate samples of the *Wall-E* video using various combination of LCD screens and camcorders. The x-axis has been mapped to Hertz (Hz) using the knowledge of the frame rate $\mathrm{f_c}$. The estimated temporal frequency $\mathrm{f_t}$ of the flicker signal is indicated for reference.



(a) (b) (c) (d)

Figure 3: Evolution of the flicker phase, computing using the Fourier coefficients $\mathbf{R}[y, \omega_t]$, with the row index in the video frame. The measurements have been extracted from camcorded recordings of the *Wall-E* video using different screen–camcorder pairs.

identifying which combination of screen–camcorder could produce such flicker. While the number of rows H in a video frame is readily available, estimating the vertical radial frequency ω_y of the flicker is more challenging. The task is complicated by the fact that the flicker signal has usually a much lower energy than the pirate video content. As a result, the video content is likely to interfere with the estimation process that only cares about the underlying flicker signal. In the next two subsections, we describe two alternate methods to estimate ω_y.

3.1 Flicker Phase Method

A first strategy to estimate the vertical radial frequency ω_y operates in two steps. The objective is to first get access to the temporal radial frequency ω_t in order to derive the vertical one from the evolution of the phase at this specific frequency.

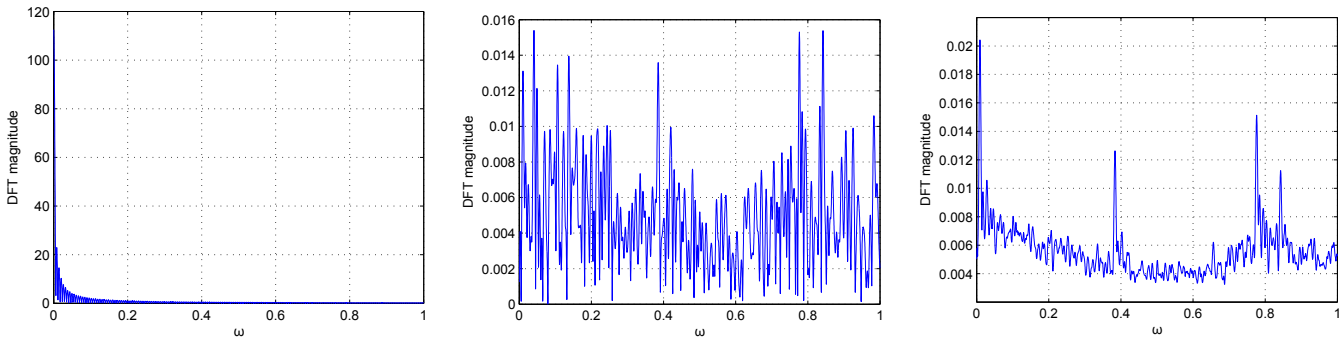
To begin with, we first compute, for each frame, the average luminance of each row:

$$\begin{aligned} \mathbf{r}[y,t] &= \frac{1}{W}\sum_{x=1}^{W}\mathbf{p}[x,y,t] \\ &= \frac{1}{W}\sum_{x=1}^{W}\left(\mathbf{c}[x,y,t]+\mathbf{f}[x,y,t]\right), \end{aligned} \tag{5}$$

where W is the number of pixels per row in a frame of the pirate sample $\mathbf{p}$. Due to its horizontal nature, this operation attenuates the interference from the content while leaving the flicker signal untouched [14, 1]. According to the model of the flicker given in Equation (1), the magnitude $\mathbf{R}[y, \omega]$ of the Fourier transform of the row average along the time axis is expected to feature a peak close to ω_t. For reference, Figure 2 illustrates this tell-tale flicker component for a variety of LCD screens and camcorder combinations. To estimate ω_t, we therefore record the radial frequency which maximizes the magnitude $\mathbf{R}[y^*, \omega]$ for any arbitrarily selected row y^*. In practice, we usually rely on a row toward the middle of the video frames to avoid unexpected behavior at the borders. To account for the fact that the low frequency range of the spectrum is likely to be dominated by the contribution of the visual content $\mathbf{c}$, the frequency range $[0, \alpha]$ is ignored during the estimation. Our empirical observations indicate that setting $\alpha = 0.4$ radians/frame manages to avoid interference from the video content in most cases.

According to Equation (1), the phase $\Phi_{\omega_t}[y]$ of the Fourier coefficients $\mathbf{R}[y, \omega_t]$ is given by $\omega_y y + \Phi_t$, with Φ_t being a time-dependent phase offset. In other words, the phase of the flicker is expected to evolve linearly along the rows, with a slope equal to the vertical radial frequency ω_y. Empirical observations reported in Figure 3 clearly indicated that it is indeed the case even if the modulo-2π operator disrupts the overall linear trend. To compensate for such undesired wrapping, the phase $\Phi_{\omega_t}[y]$ of $\mathbf{R}[y, \omega_t]$ is post-processed as follows:

$$\Psi_{\omega_t}[y] = \begin{cases} \Phi_{\omega_t}[y], & \text{if } y = 0, \\ \Psi_{\omega_t}[y-1] + d_y, & \text{if } y > 0, \end{cases} \tag{6}$$



(a) $|\mathbf{R}[\omega, t^*]|$ (b) $|\bar{\mathbf{R}}[\omega, t^*]|$ (c) $|\mathbf{S}[\omega]|$

Figure 4: Spectrum of the signal of interest at various stages of the content cancellation method. The spectrum $|\mathbf{R}[\omega, t^*]|$ of the row luminance signature (a) is dominated by the visual content and the flicker signal is not visible. In contrast, the cleaning process (b) reveals the peak corresponding to the flicker at 0.009 rad/row although it lies hidden amongst other noise components. After aggregation, the flicker frequency peak clearly appears thanks to the signal-to-noise ratio reduction.

where

$$d_y = \Big(\big(\Phi_{\omega_t}[y] - \Phi_{\omega_t}[y-1] + \pi \big) \mod 2\pi \Big) - \pi. \quad (7)$$

Estimating the vertical radial frequency ω_y is then only a matter of applying linear regression to the *unwrapped* flicker phase $\Psi_{\omega_t}[y]$ and recording the slope. As exemplified in Figure 3, the slope of the flicker phase can be positive or negative. As a result, the vertical radial frequency ω_y is simply taken as the absolute value of the estimated slope of the flicker phase.

It should be noted that the regression error provides an efficient indicator to evaluate whether the selected temporal frequency ω_t is related to a flicker or not. In some cases, the largest frequency component in $\mathbf{R}[y^*, \omega]$ is not associated to the flicker signal, which may be present in the spectrum but with a lower amplitude. In this situation, the phase $\Phi_{\omega_t}[y]$ is unlikely to be linear and the linear regression yields large error. The algorithm can then either re-run the phase regression analysis for another secondary peak of the spectrum $\mathbf{R}[y^*, \omega]$ or fall back on the alternate estimation method described hereafter.

3.2 Content Cancellation Method

The phase flicker method presented in the previous section is essentially a two-step procedure that relies on the ability to estimate the temporal radial frequency ω_t to begin with. However, in practice, such estimation may prove difficult, if not impossible. For instance, when the back-light frequency of the display apparatus gets close to a multiple of the acquisition frame rate of the camcorder, the observed aliased temporal flicker frequency appears near zero which precludes accurate estimation due to the dominance of the content in the low frequency band.

In such cases, it is necessary to rely on a fall-back estimation technique to get access to the desired vertical radial frequency ω_y. In essence, the baseline idea is (i) to clean several observations of the vertical flicker to reduce the interference from the visual content, (ii) compute the vertical spectrum of the cleaned observations, (iii) aggregate these spectra to reduce the flicker signal-to-noise ratio, and (iv) estimate the vertical radial frequency using frequency analysis.

The row luminance signatures $\mathbf{r}[y, t]$ are essentially dominated by content, thereby making the analysis of the subtle changes revealing the flicker difficult to analyze. Nevertheless, the content interference is expected to vary slowly along the rows. It is thus possible to cancel this component by applying a high-pass filter or removing the trend of the signal using some fitting tool, e.g.:

$$\bar{\mathbf{r}}[y, t^*] = \mathrm{h}\left(\mathbf{r}[y, t^*]\right), \quad (8)$$

where t^* is an arbitrarily selected time index and h(.) is any generic signal processing primitive to remove the low frequency components of a signal. Empirical observations indicate that this cleaning process is more efficient for uniform frames having more predictable row luminance signatures.

Still, significant content energy usually remains in individual cleaned row luminance signatures. As a result, estimating the vertical radial frequency ω_y based on the spectrum analysis of a single row luminance signature, even cleaned, may be unsuccessful. To improve the signal-to-noise ratio, it is common practice in multimedia security to aggregate several observations to reduce the interference introduced by uncorrelated noise components [6, 10]. Such aggregation can be performed directly in the Fourier domain:

$$|\mathbf{S}[\omega]| = \frac{1}{M} \sum_{i=1}^{M} |\bar{\mathbf{R}}[\omega, t_i]|, \quad (9)$$

where $|\bar{\mathbf{R}}[\omega, t^*]|$ is the magnitude of the Fourier transform of the cleaned row luminance signature $\bar{\mathbf{r}}[\omega, t^*]$, $|\mathbf{S}[\omega]|$ the magnitude of the vertical flicker spectrum, and the set of time indices $\{t_i\}_{1 \le i \le M}$ indicate which frames of the video sequence have been incorporated into the aggregation. In practice, we considered the $M = 40$ most uniform video frames, i.e. the M frames with the lowest variances, since empirical observations reveal that they provide better vertical flicker estimates $\bar{\mathbf{r}}[y, t^*]$.

Eventually, the vertical radial frequency ω_y is given by the frequency whose magnitude is maximal in the spectrum $|\mathbf{S}[\omega]|$. In this paper, to avoid false estimations, we also discard frequencies $\omega > \beta$ since they correspond to back-light

frequencies that are never used in practice. Our empirical observations showed that using $\beta = 1$ radians/row provides good performances in general. For reference, Figure 4 depicts the added value of the cleaning and aggregation processes in a particularly difficult case.

4. FORENSIC INVESTIGATIONS

In this paper, a typical forensic scenario is that law enforcement forces have searched the homes of suspected pirates and seized camcorded movie samples as well as a collection of screens and camcorders. A key question is then to establish whether these suspect devices could have produced the collected pirate multimedia material. The charges against piracy consumers and piracy producers are indeed not the same.

In the remainder of the article, we investigate if flicker-based forensic analysis could successfully achieve this identification task. For completeness, we survey three alternate use cases corresponding to different a priori knowledge about the pirate devices. For the time being, we assume that we can have access to the read-out time T_{ro} of a camcorder and the back-light frequency f_{BL} of an LCD screen. We will detail in Section 5 how to retrieve these values in practice.

4.1 Camcorder Identification

In this scenario, the pirate LCD screen is assumed to be known and the forensic task therefore reduces to identifying the pirate camcorder within a collection of suspect devices. Based on the piracy identity given by Equation (4), it is immediate to write:

$$T_{\text{ro}} = \frac{H \cdot \omega_y}{2\pi \cdot f_{\text{BL}}}. \tag{10}$$

The frame height H can be directly accessed from the pirate video and the vertical radial frequency ω_y can be estimated using any of the two methods described in Section 3. Since the pirate screen is assumed to be known, we have access to f_{BL} and we can compute the read-out time T_{ro} of the camcorder used to produce the pirate video sample. Pinpointing the pirate camcorder amongst the set of suspect devices is then simply a matter of identifying the device whose read-out time is the closest to this target value.

4.2 Screen Identification

Conversely, we can assume that the pirate camcorder is known and that the objective is to pinpoint the pirate screen amongst several suspect devices. Still reusing Equation (4), it is straightforward to express the back-light frequency as:

$$f_{\text{BL}} = \frac{H \cdot \omega_y}{2\pi \cdot T_{\text{ro}}}. \tag{11}$$

As previously, we can rely on the parameters derived from the pirate video and camcorder to compute the pirate back-light frequency. The identification task then amounts to finding the screen whose back-light frequency is the closest to this target value.

While this strategy does provide an estimate of the back-light frequency f_{BL}, it relies on the estimation of the vertical radial frequency ω_y which may be very rough, especially when using the content cancellation method. As a result, the forensic identification accuracy may be jeopardized. In order to mitigate this limitation, instead of trying to identify the characteristic, it may be advantageous to simply verify if a pair of suspect devices could produce the flicker signal observed in the pirate movie in a matter similar to what is done in biometrics.

For instance, considering a potential pair of pirate devices, it is possible to derive the theoretical aliased frequency f_t based on the back-light frequency f_{BL} of the screen and the sampling rate f_{c} of the camcorder. As a result, in the flicker phase method, instead of blindly looking for the temporal radial frequency ω_t in the spectrum $\mathbf{R}[y^*, \omega]$, we can restrict the search within a small range around the theoretical flicker aliased frequency. First, it allows to accurately lock on frequencies which may have been overlooked by mistake for not having the global maximum magnitude of the spectrum. Second, it provides means to quickly discard suspect pairs of devices when the phase $\Phi_{\omega_t}[y]$ is found not to be linear.

On another front, we could exploit the knowledge of the parameters of the suspect devices to improve the estimation accuracy of the back-light frequency. Based on the estimation of the temporal radial frequency ω_t, which has been empirically found to be more accurate than ω_y, it is possible to refine the estimation of the back-light frequency, e.g.:

$$f_{\text{BL}}^{\dagger} = \Big| f_t + f_{\text{c}} \cdot \arg\min_{k \in \mathbb{Z}} \big| f_{\text{BL}} - |f_t + k \cdot f_{\text{c}}| \big| \Big|. \tag{12}$$

In other words, we exploit the aliasing phenomenon to identify which candidate frequency $|f_t + k \cdot f_{\text{c}}|$, $k \in \mathbb{Z}$, is the closest to the rough estimation obtained in Equation (11).

4.3 Blind Identification

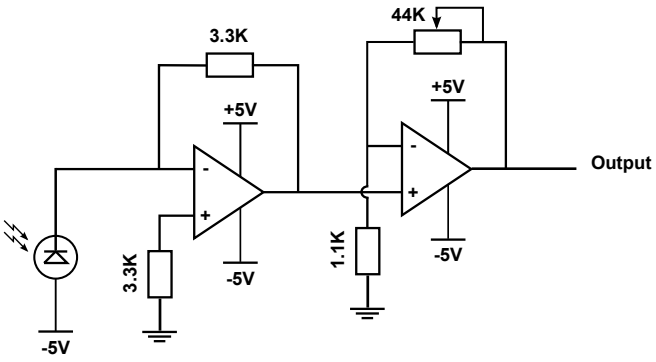
In the most challenging scenario, neither the pirate screen nor the pirate camcorder have been yet identified and the forensic analyst has to investigate the pirate video in a completely blind manner. As a matter of fact, she is reduced to evaluating both sides of the piracy identity, duplicated here for convenience:

$$T_{\text{ro}} \cdot f_{\text{BL}} = \frac{H \cdot \omega_y}{2\pi}.$$

The product on the left-hand side can be evaluated using the ground truth back-light frequency and read-out time retrieved from the pirate devices. The left-hand side can be computed by analyzing the flicker signal present in the camcorded pirate video sequence. Identifying the pirate devices among a collection of suspect LCD screens and camcorders is then simply a matter of isolating the pair of devices which yields a difference between the two sides of the piracy identity that is the closest to zero.

5. PIRATE DEVICES CHARACTERISTICS

As described in the previous section, the proposed forensic protocol heavily relies on the ability of the analyst to have access to the characteristics of the suspect devices, namely the back-light frequency f_{BL} of the LCD screens and the read-out time T_{ro} of the camcorders. Unfortunately, such low-level characteristics are usually not indicated in the datasheets or manuals of consumer electronics products. Moreover, these parameters may differ along the production line and it is therefore preferable to extract the ground truth parameters from the suspect devices seized during the investigation. In contrast with the forensic analysis of the pirate video sequence, the extraction of these parameters is performed in a controlled environment e.g. devices can



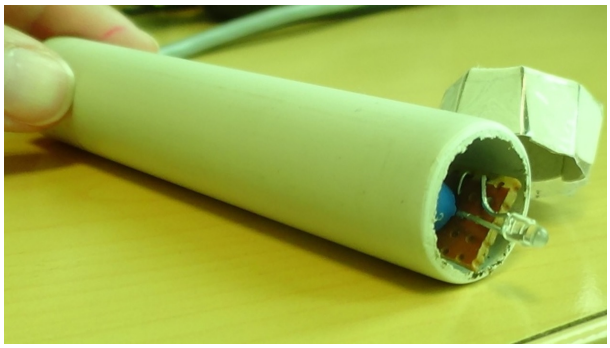


Figure 5: Custom-made light sensing probe. The photo-diode converts light into electric current, which is amplified by a first amplifier on the left-hand side. Namely, 0.1 mW/cm^2 yields a current of 0.8 μA and 2.64 mV. The adjustable gain amplifier on the right-hand side is then useful for accommodating to various light intensities of different screens. The gain can vary between 1 and 44.

Table 1: LCD screens used in our experiments

ID	Brand	Model	f_{BL} (Hz)
1	Dell	2209WA	240.06
2	Dell	U2410	180.43
3	Samsung	LE37B652T4WXXC	159.98
4	Samsung	UE32C6000RWXZF	120.00
5	Sony	KDL-32P3000	146.61
6	Sony	KDL-37P3000	226.70
7	Sony	KDL-32W5710	172.80

be fed with specific stimuli to facilitate measurements. The only constraint is to avoid tampering with the integrity of the device, i.e. breaking apart the device to examine its individual components.

5.1 LCD Screen Back-light Frequency

To reverse engineer the back-light frequency of an LCD screen in a non-invasive way, the first task is to get access to the raw signal with some kind of probe. To do so, we custom-made a sensing circuit that converts captured light into an electrical signal. In a nutshell, the reversed-current of a photo-diode is amplified with a regular transistor. The whole circuit is embedded within a pen-like casing that has a pin hole to let incoming light in as illustrated in Figure 5. The output of the sensing circuit can then be connected to a PC or an oscilloscope for live analysis or to some recording device, e.g. an audio recorder, for off-line analysis. By placing this apparatus on the surface of a screen which displays a static uniform gray frame, it gets direct access to the back-light signal without interference from other light sources or from the temporal dynamic of a motion picture. The recorded signal is typically a periodic signal whose fundamental frequency is equal to the back-light frequency f_{BL} of the LCD screen. Straightforward spectrum analysis then allows to efficiently extract the ground truth back-light frequency of the screen. In Table 1, we report on the measurements obtained on the seven LCD screens used in our experiments. The reverse-engineered back-light frequencies are within a 120-250 Hz which is in line with the known practices of the display industry.

Table 2: Camcorders used in our experiments

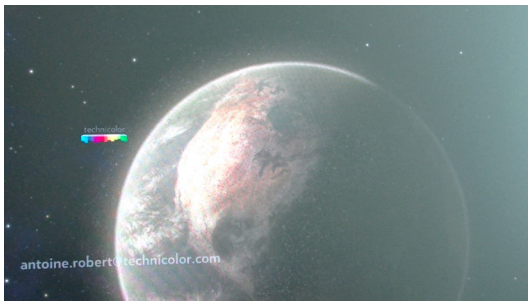
Brand	Model	f_{c} (fps)	H	T_{ro} (ms)
JVC	GC-PX100BE	50	1080	13.5
Panasonic	HDC-SDT750	50	1080	16
Sony	HDR-CX200E	25	540	15
Toshiba	PA5081E-1C0K	29.97	1080	32.65

5.2 Camcorder Read-out Time

Getting access to the read-out time T_{ro} of a camcorder is less direct than measuring the back-light frequency using a probe. The trick is to record a reference LCD screen displaying gray scale content, as depicted in Figure 1, with the suspect camcorder to obtain a short video sequence (e.g. 30 seconds) where the flicker is apparent. Based on our ability to extract the ground truth back-light frequency of the reference screen and thanks to the lack of visual content interference since we are using a neutral stimulus, the flicker phase method described in Section 3.1 provides access to the vertical radial frequency ω_y of the flicker which in turn yields the desired read-out time using Equation (10). To avoid corner cases where temporal aliasing may interfere with the estimation of ω_y, several reference screens may be considered to be more confident of the computed read-out time. The measurements that we obtained with the four camcorders used in our experiments are reported in Table 2 for reference. It should be noted that all camcorders are progressive, except the Sony camera which is interlaced. For convenience, we simply kept one of the two fields for this camera, thereby resulting in a vertical resolution of 540 rows although the camcorder has the ability to capture 1080 rows.

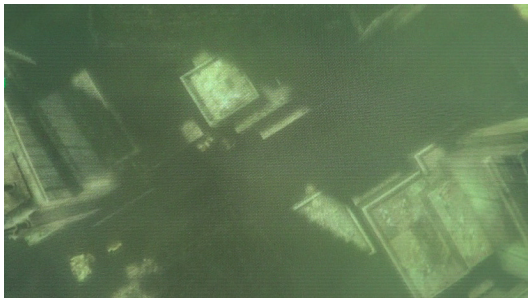
6. EXPERIMENTAL RESULTS

To validate our forensic protocol based on the analysis of the flicker signal present in camcorded pirate videos, we constructed a dedicated experimental dataset. For all combinations of LCD screens and camcorders from the pool of devices listed in Tables 1 and 2, we recorded a 1 minute long video sequence taken from the opening scene of the movie *Wall-E* displayed on a screen. Figure 6 depicts some screenshots for such camcorded video sequences. It is important

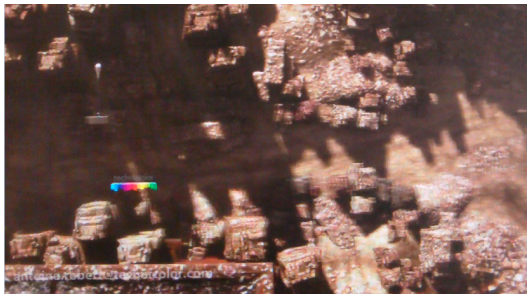


(a) `Screen 2` and `JVC`

(b) `Screen 3` and `Panasonic`



(c) `Screen 7` and `Sony`



(d) `Screen 1` and `Toshiba`

Figure 6: Screenshots of camcorded video sequences using various screen–camcorder pairs. Besides very different color changes, the flicker signal is more or less apparent depending on the pair of pirate devices.

Table 3: Aliased temporal frequency f_t either computed from the ground-truth measurement of the back-light frequency f_{BL} of the pirate LCD screen or estimated from the pirate video samples

	f_{BL}	JVC		Panasonic		Sony		Toshiba	
	(Hz)	**Theo.**	**Exp.**	**Theo.**	**Exp.**	**Theo.**	**Exp.**	**Theo.**	**Exp.**
`Screen 1`	240.06	9.94	9.94	9.94	9.94	9.94	9.94	0.30	*N/A*
`Screen 2`	180.43	19.57	19.56	19.57	19.56	5.43	5.44	0.61	*N/A*
`Screen 3`	159.98	9.98	9.99	9.98	9.99	9.98	9.99	10.13	10.13
`Screen 4`	120.00	20.00	20.02	20.00	19.97	5.00	4.98	0.12	*N/A*
`Screen 5`	146.61	3.39	3.39	3.39	3.47	3.39	3.39	3.24	3.48
`Screen 6`	226.70	23.30	23.34	23.30	23.32	1.70	*N/A*	13.06	12.82
`Screen 7`	172.80	22.80	22.80	22.80	22.80	2.20	2.20	7.02	7.02

to note that the flicker is not always very visible but that, as will be detailed in the next sections, it can still be exploited to extract the desired forensic information. Overall, the experimental dataset amounts to 28 camcorded videos and we report hereafter the identification performances depending on the considered forensic scenario.

6.1 Camcorder Identification Scenario

When estimating the vertical radial frequency ω_y from the pirate video sample using the flicker phase method described in Section 3.1, a key intermediary step is the accurate estimation of the temporal frequency ω_t. For reference, we report in Table 3 the theoretical values obtained from the ground-truth measurements of the back-light frequency f_{BL} as well as the values obtained experimentally from the video samples. For ease of interpretation, these values are provided in Hertz, assuming knowledge of the camera acquisition rate f_c. Most of the aliased temporal frequency estimates are very close to the expected theoretical values, e.g. within a range of ± 0.02 Hz. This very high accuracy validates the refinement procedure proposed in Section 4.2. Still, in four cases, the flicker phase method is unsuccessful. Essentially, the aliased temporal frequency f_t is too close to the content-dependent low-frequency components. Visually, it translates as a static flicker signal, i.e. horizontal strips of varying luminance with marginal vertical drift. In such cases ($\omega_t < \alpha$), there is no other choice but to fall back on the backup estimation method even if it yields less accurate estimates of the vertical radial frequency ω_y.

Once the vertical radial frequency ω_y is estimated, obtaining the read-out time T_{ro} of the pirate camcorder is simply a matter of applying Equation (10), using the back-light frequency f_{BL} of the known pirate LCD screen. The pirate camcorder is then the one whose ground truth read-out time is the closest to this estimated value. The experimental results reported in Table 4 indicate that the pirate camcorder is correctly identified in 25 out of 28 videos, i.e. 89% correct identification. One of the unsuccessful identification actually features an estimated read-out time much larger than the ground truth value, namely 63.77 ms vs. 16 ms. In this par-

Table 5: Back-light frequency f_{BL} computed either by leveraging on the piracy identity with Equation (11) or by exploiting frequency aliasing to refine the rough estimate with Equation (12). Figures in italic indicate LCD screen identification errors.

	f_{BL}	JVC		Panasonic		Sony		Toshiba	
	(Hz)	**Rough**	**Refined**	**Rough**	**Refined**	**Rough**	**Refined**	**Rough**	**Refined**
Screen 1	240.06	243.22	240.06	238.18	240.06	240.46	240.06	241.26	N/A
Screen 2	180.43	177.74	180.44	178.46	180.44	181.08	180.44	179.68	N/A
Screen 3	159.98	159.36	159.99	158.33	159.99	156.90	159.99	159.94	159.98
Screen 4	120.00	115.67	120.02	*238.64*	*240.01*	112.69	120.01	119.12	N/A
Screen 5	146.61	145.49	146.61	136.73	146.53	146.60	146.61	147.57	146.37
Screen 6	226.70	225.83	226.66	227.67	226.68	226.32	N/A	227.02	226.94
Screen 7	172.80	173.48	172.80	172.39	172.80	173.00	172.80	171.82	172.80

Table 4: Frame read-out times T_{ro} estimated from pirate video sequences obtained using various pirate camcorder-screen pairs. Figures in italic highlight pirate camcorder identification mistakes.

	JVC	Panasonic	Sony	Toshiba
T_{ro} **(ms)**	13.5	16	15	32.65
Screen 1	13.68	15.87	15.03	32.81
Screen 2	13.30	15.82	15.05	32.52
Screen 3	13.45	15.83	14.71	32.64
Screen 4	13.01	*63.77*	*14.09*	32.41
Screen 5	13.40	*14.92*	15.00	32.86
Screen 6	13.45	16.07	14.97	32.70
Screen 7	13.55	15.96	15.02	32.47

Table 6: Identified pirate screen–camcorder pairs with the video sequences of our dataset. Pirate devices are represented by the format [J,P,S,T]–[1...7], where the letter indicates the camcorder and the number the LCD screen. Entries in italic highlight identification errors.

	JVC	Panasonic	Sony	Toshiba
Screen 1	J–1	P–1	S–1	T–1
Screen 2	*S–3*	P–2	S–2	T–2
Screen 3	J–3	P–3	*P–5*	T–3
Screen 4	J–4	*P–1*	*J–4*	T–4
Screen 5	J–5	*S–5*	S–5	T–5
Screen 6	J–6	P–6	S–6	T–6
Screen 7	*P–5*	P–7	S–7	T–7

ticular case, the back-light frequency of the screen is 120 Hz and is thus aliased to $|120 - 2 \times 50| = 20$ Hz when using the Panasonic camcorder. However, the fourth harmonic of the back-light also aliases at $4 \times 120 - 10 \times 50 = 20$ Hz. As a result, when the flicker phase method looks at the phase at frequency $f_t = 20$ Hz, it picks up the fourth harmonic and thereby overestimates the read-out time by a factor of 4. Should we divide the estimated value by 4, we would obtain $T_{ro} = 15.94$ ms and thus correctly estimate the Panasonic camcorder. The other two errors simply indicate the current limitation of the proposed forensic strategy when the visual content interferes with the estimation process.

6.2 Screen Identification Scenario

As discussed in Section 4.2, it is possible to estimate the back-light frequency f_{BL} of the pirate LCD screen by applying Equation (11) obtained by manipulating the piracy identity which links the vertical radial frequency of the pirate video sequence and the characteristic parameters of the pirate devices. Table 5 lists such rough estimates extracted from the video sequences in our experimental dataset. While the estimation is reasonably accurate, it sometimes yields notable deviation, e.g. the 10 Hz bias with the Panasonic camcorder and the Screen 5, which could result in identification mistakes. The a priori knowledge about the pirate camcorder grants the opportunity to leverage on the frequency aliasing mechanism to obtain a refined estimation of when an estimate of the aliased temporal frequency f_t is available. The refined estimates listed in Table 5 clearly showcase the improved accuracy of the estimation. All refined back-light frequency estimates are indeed within a 1 Hz error margin around the ground truth except for a single combination of camcorder-screen pirate devices. In other words, pirate LCD screen identification is successful for 27 out of 28 pirate sequences.

As in a previous scenario, the combination of the Panasonic camcorder and the Screen 4 appears to be a corner case. Interestingly, though, the problem does not only come from the fact that the fundamental and fourth harmonic of the back-light signal overlap at 20 Hz. When analyzing this pirate video sequence, each screen is successively tested as a potential pirate device. In particular, Screen 1 and Screen 3 are expected to have an aliased temporal frequency f_t close to 10 Hz with the Panasonic camcorder. On the other hand, 10 Hz is also the location of the second harmonic ($2 \times 120 - 5 \times 50 = 10$) for Screen 4. As a result, the forensic analysis will reveal two candidate f_t values at 10 Hz and 20 Hz, each one having a linear phase $\Phi_{\omega_t}[y]$ and associated to two estimates of ω_y corresponding to 240 Hz and 480 Hz respectively. It is common practice to eliminate higher harmonics and the algorithm therefore outputs 240 Hz, mistaking Screen 1 for the pirate LCD screen.

6.3 Blind Identification Scenario

When there is no a priori information on the pirate devices, all potential screen–camcorder pairs have to be evaluated. The forensic protocol reduces in this case to the evaluation of the left-hand side and the right-hand side of the piracy identity given by Equation (4) and to isolate the pair of devices which yields the lowest difference. The results of such blind identification of the pirate devices are reported in Table 6. As could be anticipated, the lack of a priori in-

Table 7: Flicker forensics accuracy

Scenario	Accuracy
Camcorder Identification	89%
Screen Identification	96%
Blind Identification	79%

formation naturally translates in reduced identification accuracy. Still, the proposed forensic protocol is successful in 22 cases out of 28, i.e. a 79% correct identification rate.

When looking closely at the six identification mistakes, it is possible to isolate two main sources of error. First of all, the three entries with errors in Table 4, which are also the ones whose back-light frequency estimation error is among the largest in Table 5, produce errors in the blind identification scenario. In other words, pirate sequences which provide incorrect results in the non-blind scenarios, due to the limitations of the methods proposed to estimate the radial vertical frequency ω_y, also produce errors in more challenging forensic conditions.

The second source of error originates from the fact that screen–camcorder pairs are reduced to the product $\Pi = T_{\text{ro}} \cdot f_{\text{BL}}$ between the frame read-out time of the camcorder and the back-light frequency of the LCD screen. As a result, alternate screen–camcorder pairs may have very similar characteristic Π values. This is in particular the case for the pairs J–2, J–7, S–3, and P–5 which all have $\Pi \approx 2480 \pm 50$. These devices are thus considered close to equivalent during the forensic analysis and slight estimation errors for ω_y may lead to a screen–camcorder pair being confused for another one.

7. CONCLUSIONS AND FUTURE WORK

In this paper, we presented a passive forensic methodology to characterize pirate video sequences which have been created by placing a camcorder in front of an LCD screen displaying content. In essence, the idea is to isolate the flicker signal originating from the interplay between the screen's back-light and the camcorder's shutter and use it to verify which screen–camcorder pair, among a collection of devices, can produce such a visual artifact. To do so, we presented a number of estimation methods to characterize the flicker as well as some non-invasive measurement protocols to recover ground-truth parameters of the devices. Flicker-based pirate device attribution performances are summarized in Table 7 for the different forensic scenarios that we have considered in this study. While imperfect, they clearly demonstrate the potential for the flicker signal to serve as a powerful complementary tell-tale forensic indicator for pirate video samples. It could prove very useful for instance to establish piracy links between unrelated pirate video sequences for instance.

In future work, we intend to first focus on improving the estimation techniques to estimate f_t and ω_y since they have been found to significantly impact identification performances. For instance, we will investigate how to better exploit the harmonics of the flicker signal both to eliminate spurious peaks in the spectrum or to consolidate the estimation of the vertical radial frequency across various frequency bins. Although our preliminary investigations indicated that flicker forensics is barely affected by subsequent video processing, we will further benchmark the robustness of the proposed estimation techniques to better appreciate the operating region of our system. Eventually, we will also look for additional statistical footprints in pirate movies that may involve other parameters of the screen/camcorder. This will be most helpful to introduce diversity among screen-camcorder pairs which have equivalent $\Pi = T_{\text{ro}} \cdot f_{\text{BL}}$ values that may be confused for one another.

An important thing to keep in mind, though, is that the parameters inducing the statistical footprint in the camcorded video should ideally be intrinsic to the device. Indeed, the beauty of the back-light frequency of an LCD screen and the frame read-out time of a camcorder is that they cannot be modified by the user. In contrast, while Moiré patterns present in camcorded videos may reveal information about the interaction between pirate devices, they are dependent on the acquisition geometry and are thus unlikely to be useful for device identification.

8. ACKNOWLEDMENTS

The authors would like to thank Mario de Vito for designing and building the custom-made sensing probe that we used in our experiments.

9. REFERENCES

[1] S. Baudry, B. Chupeau, M. de Vito, and G. Doërr. Modeling the flicker effect in camcorded videos to improve watermark robustness. In *Proceedings of the IEEE Workshop on Information Forensics and Security*, pages –, December 2014.

[2] N. Chang, I. Choi, and H. Shim. DLS: Dynamic backlight luminance scaling of liquid crystal display. *IEEE Transactions on Very Large Scale Integration*, 12(8):837–846, August 2004.

[3] B. Chupeau, S. Baudry, and G. Doërr. Forensic characterization of pirated movies: Digital cinema cam vs. optical disc rip. In *Proceedings of the IEEE Workshop on Information Forensics and Security*, pages –, December 2014.

[4] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker. *Digital Watermarking and Steganography*. Morgan Kaufmann Publishers Inc., 2nd edition, 2008.

[5] Digital Cinema Initiatives, LLC. *Digital Cinema System Specification*, 1.2 edition, March 2008.

[6] G. Doërr and J.-L. Dugelay. Security pitfalls of frame-by-frame approaches to video watermarking. *IEEE Transactions on Signal Processing*, 52(10):2955–2964, October 2004.

[7] T. Furon and G. Doërr. Tracing pirated content on the internet: Unwinding Ariadne's thread. *Security & Privacy*, 8(5):69–71, September/October 2010.

[8] A. E. Gamal and H. Eltoukhy. CMOS image sensors. *IEEE Circuits & Devices Magazine*, 21(3):6–20, May/June 2005.

[9] C.-K. Liang, L.-W. Chang, and H. H. Chen. Analysis and compensation of rolling shutter effect. *IEEE Transactions on Image Processing*, 17(8):1323–1330, August 2008.

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

[11] J. J. Moreira-Pérez, B. Chupeau, S. Baudry, and G. Doërr. Exploring color information to characterize camcorder piracy. In *Proceedings of the IEEE Workshop on Information Forensics and Security*, pages 132–137, November 2013.

[12] MovieLabs. MovieLabs specifications for next generation of video and enhanced content protection. Technical report, 2013. `http://www.movielabs.com/ngvideo/`.

[13] D. Poplin. An automatic flicker detection method for embedded camera systems. *IEEE Transactions on Consumer Electronics*, 52(2):308–311, May 2006.

[14] X. Rolland-Nevière, B. Chupeau, G. Doërr, and L. Blondé. Forensic characterization of camcorded movies: Digital cinema vs. celluloid film prints. In *Media Watermarking, Security, and Forensics*, volume 8303 of *Proceedings of SPIE*, January 2012.

[15] W. Rosenblatt, S. Mooney, and W. Trippe. *Digital Rights Management: Business and Technology*. John Wiley & Sons, Inc., 2001.

[16] Y. Yoo, J. Im, and J. Paik. Flicker removal for CMOS wide dynamic range imaging based on alternating current component analysis. *IEEE Transactions on Consumer Electronics*, 60(3):294–301, August 2014.