Tempest in a Teapot: Compromising Reflections Revisited

Michael Backes[*†], Tongbo Chen[‡], Markus Dürmuth[*], Hendrik P. A. Lensch[§], and Martin Welk[*]
[*] *Saarland University, Saarbrücken, Germany,*
{backes | duermuth}@cs.uni-sb.de, welk@mia.uni-saarland.de
[†] *MPI SWS, Saarbrücken, Germany*
[‡] *MPI Informatik, Saarbrücken, Germany, tongbo@mpi-inf.mpg.de*
[§] *Ulm University, Germany, hendrik.lensch@uni-ulm.de*

Abstract

Reflecting objects such as tea pots and glasses, but also diffusely reflecting objects such as a user's shirt, can be used to spy on confidential data displayed on a monitor. First, we show how reflections in the user's eye can be exploited for spying on confidential data. Second, we investigate to what extent monitor images can be reconstructed from the diffuse reflections on a wall or the user's clothes, and provide information-theoretic bounds limiting this type of attack. Third, we evaluate the effectiveness of several countermeasures. This substantially improves previous work (Backes et al., IEEE Symposium on Security & Privacy, 2008).

1. Introduction

Emanations leaking potential confidential information, emitted by computers and similar devices, have been a topic of concern for a long time. Although the military had prior knowledge [34], [15], by 1985, techniques to use the electromagnetic emanation of CRT monitors to reconstruct the monitor's content were publicly known [32]. This approach was further refined, and similar attacks emerged, e.g., capturing the monitor's content from the emanation of the cable connecting the monitor and the computer [16].

In [4], the authors presented a novel method to exploit the optical, i.e., the unavoidable emanation of *every* monitor, not just CRT monitors. They demonstrated how to exploit tiny reflections in a large variety of stationary objects that are typically located in every office to spy on confidential data displayed on a computer monitor. Astronomic telescopes and digital cameras are employed in this approach. While the idea is seemingly simple, capturing images of high resolution over large distances is not easy and limited by physical phenomena, in particular by diffraction.

What makes the attack based on observing reflections particularly interesting is that (i) it exploits emanations that are not a side-product of computation such as electromagnetic emanations but are part of the normal operation, and (ii) it works with *any* type of monitor. In fact, this attack is the only known attack that applies to today's typical environments, where CRT monitors are replaced by TFT monitors and electromagnetic radiation can be (and in highly-sensitive areas actually *is*) shielded.

1.1. Our Contributions

Previous work, however, still relies on the presence of stationary reflecting objects. If there are no such objects, is privacy guaranteed? We show that this is not the case. First, we investigated reflections in the user's eye and show that these reflections can be exploited as well. Second, we investigated diffuse reflections from a wall or a shirt that can be used to reconstruct the monitor image.

Capturing reflections from the human eye is particularly interesting, as the eye is present in essentially any environment were sensitive information is displayed. It thus poses a threat much more difficult to mitigate. While [4] mentions this possibility, they were unable to capture more than basic shapes from reflections in the eye (cf. Figure 1).

We fundamentally improve their results (cf. Figure 2). For the human eye, we can read 36pt font from a distance of 10 meters, while previously only 150pt font was readable from a distance of four meters.

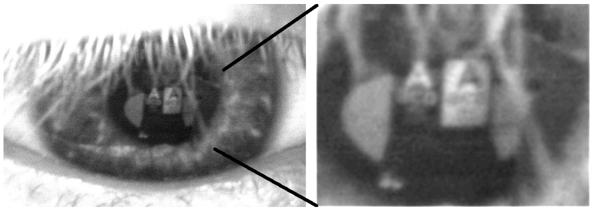

Figure 1. Previous results from [4]: Reflections in the eye from 4 meters.

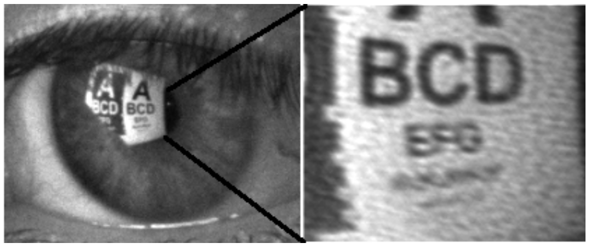

Figure 2. Our results: Reflections captured in the eye from a distance of 10 meters.

Furthermore, we see that the achievable distance scales linearly in the main limiting parameter, the telescope diameter. Thus we can extrapolate our results and see a linear trade-off between the attackers abilities and the required telescope sizes.

The ability to read the monitor image is limited by three types of blur: blur caused by incorrect focus (out-of-focus blur), blur caused by movement of the eye (motion blur), and blur caused by diffraction (diffraction blur). Capturing high-resolution images over a large distance typically requires the use of large focal length and large apertures. This, however, results in a very small depth-of-field, i.e., only objects that are precisely in focus appear sharp, and objects that are slightly out-of-focus are significantly blurred. Consequently, focusing is very sensitive, and *out-of-focus blur* can hardly be avoided during capture, in particular for moving objects such as the human eye. *Motion blur*, on the other hand, is caused mainly by the rapid movement of the eye. Finally, *diffraction blur* is an optical phenomenon caused by the limited aperture of the telescope. The aperture basically deletes high frequency parts of the image. This information is effectively lost, thus it cannot be reconstructed from the blurred image. (One exception occurs if there is a sufficient amount of additional information about the image, e.g., if it is known that the image of a star was captured, then the exact location of the star can be determined even in the presence of diffraction blur.)

In computer graphics, blur is described by a *point spread function (PSF)* which models the redistribution of energy from each point of the (unobservable) sharp image to each point of the blurred image. Our task thus is to reconstruct the sharp image, given a description of the PSF and the blurred image. This task is known as *(non-blind) deconvolution*.

We demonstrate how to use image deconvolution algorithms to improve the image quality. We show that both motion blur and out-of-focus blur can be efficiently removed, whereas diffraction blur cannot effectively be countered and thus constitutes a principal limitation to the applicability of the attack.

One central challenge is to measure the PSF. While there exist deconvolution algorithms that determine the PSF in the process of deconvolution (blind deconvolution), their performance is much lower than the performance of non-blind deconvolution algorithms, i.e., deconvolution algorithms that are given as extra side information the PSF. We identified and tested two practical possibilities to determine the PSF. First, we captured several PSFs that result from different levels of out-of-focus blur upfront (offline) and use this information later in deconvolution. This approach works very well if there is only out-of-focus blur present (see Section 2.4). It can, however, not handle motion blur. Therefore, we explored another approach (see Section 2.5) where we measure the PSF when we take the picture, simultaneously measuring motion blur and out-of-focus blur. This approach requires a small amount of extra hardware, but it is highly practical.

Our results get close to the diffraction limit, i.e., we are able to obtain the physical optimum. This in turns lets us eliminate the possibility of further improvements and provides a bound on the applicability of this type of attacks.

Another type of attack we explore are *diffuse reflections*. The possibility that one can spy on confidential data exploiting *diffuse reflections*, e.g., reflections on a white wall, were briefly mentioned in [4]. In this work we take a systematic approach and explore the exact possibilities of this attack and we show *information-theoretic limits* of the attack. Our approach is different from the attack presented in [14] in that the later exploits temporal variations of the diffuse reflections and thus is restricted to CRT monitors, a technology that is rarely used nowadays. Our approach uses spatial variations only and is applicable to *any* monitor technology. Ironically, the user's attempt to increase his privacy may actually lead to weaker privacy: We found that the reconstruction works better if the user is using a privacy filter to protect himself from somebody spying over his shoulder: these filters direct the light coming from the monitor, thus making the convolution kernel smaller.

Finally, we evaluated the effectiveness and applicability of several countermeasures. In particular, we showed that deploying polarization filters on the window to block the (polarized) light emitted by the monitor does not offer reasonable protection in practice. (This countermeasure was suggested by the audience at the IEEE Symposium on Security & Privacy 2008.) We propose a novel countermeasure based on optical notch filters, which conceptually provides much better protection.

While the techniques we used are considerably more involved than what was used in previous work, neither hardware nor software requirements are prohibitively expensive. Our improvements do not only affect image quality for pictures of the eye: Also reflections in other objects can be captured with much higher quality using our improved tools.

1.2. Further Related Work

Military organizations have been rumored to investigate compromising emanations since the 1960's; the results of these works, however, are confidential. The first publicly known attack we are aware of was published in 1985 [32] and used electromagnetic radiation of CRT monitors. An early discussion of these results can be found in [12].

Various forms of emanations have since been exploited to spy on confidential data. Electromagnetic emanations that constitute a security threat to computer equipment result from poorly shielded RS-232 serial lines [29], keyboards [1], as well as the digital cable connecting modern LCD monitors [16]. We refer to [17] for a discussion on the security limits for electromagnetic emanation. Acoustic emanations were shown to reveal text typed on ordinary keyboards [3], [37], as well as information about the CPU state and the instructions that are executed [28]. Acoustic emanations from printers were studied in [7]. The time-varying diffuse reflections of the light emitted by a CRT monitor can be exploited to recover the original monitor image [14]. This approach exploits the point-wise image construction and the time-characteristics of the light-emitting material used in CRT monitors and consequently does not apply to monitors that do not construct images in this fashion, such as LCD monitors. Information leakage from status LEDs is studied in [18]. Reflections of images from a human eye were already investigated prior to [4] in [20], but without security questions in mind, in particular only for low resolutions, small distances, and without proposing technical and algorithmic approaches to extend the resolution.

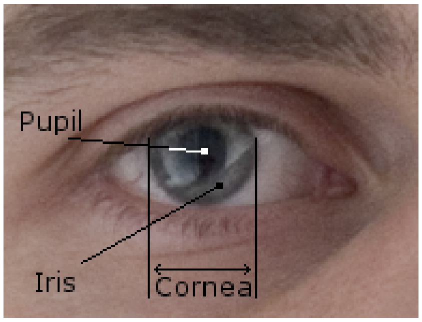

Figure 5. The human eye.

A comprehensive description of astronomic image processing, including various imaging systems, practical acquisition and advanced post-processing techniques is provided in [5]. The application of deconvolution to astronomic imaging is surveyed in [30]. The Richardson-Lucy (RL) deconvolution was described in [25], [19]. Other common (non-blind) deconvolution algorithms include van Cittert deconvolution [8] and the Wiener filter [33]. Furthermore, modified camera designs, including a synthetic high-speed shutter operated with coded temporal patterns [31] or a patterned mask at the aperture plane [24], have been proposed to counteract motion or out-of-focus blur, respectively. Yuan et al. [35] presented a technique for combining a pair of short and long exposed images to remove the motion blur from the brighter image while keeping its color fidelity.

1.3. Structure of the Paper

In Section 2 we consider reflections in the human eye. In Section 3 we describe how to reconstruct diffuse reflections and give bounds for the reconstruction. In Section 4 we show that known countermeasures do not provide reasonable protection and propose a new one to circumvent these problems. We conclude with Section 5.

2. Reflections in the Eye

The human eye produces very sharp reflections, as experiments from a short distance show. In principle, this enables us to exploit the reflections in the user's eye to spy on the monitor. However, in practice it is very difficult to capture these reflections: noise and blur substantially reduce the image quality. First, the eye's strong curvature (the cornea of a typical human eye has

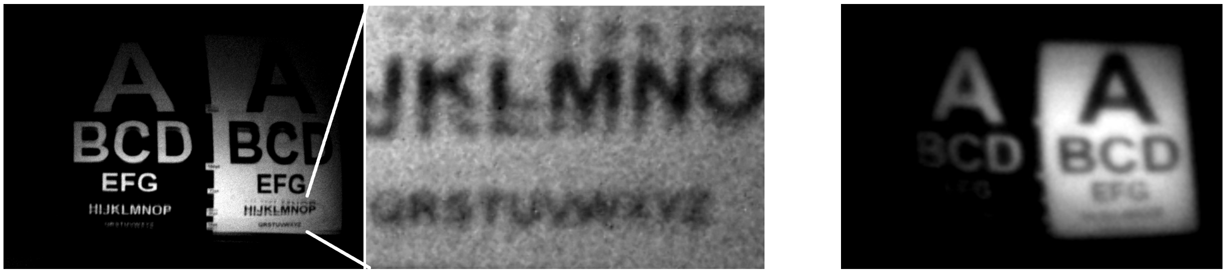

Figure 3. Previous results from [4]: Reflections in a tea pot from a distance of 10 meters (left) and 40 meters (right), respectively, using a 20cm Dobson and the Canon EOS 400D camera.

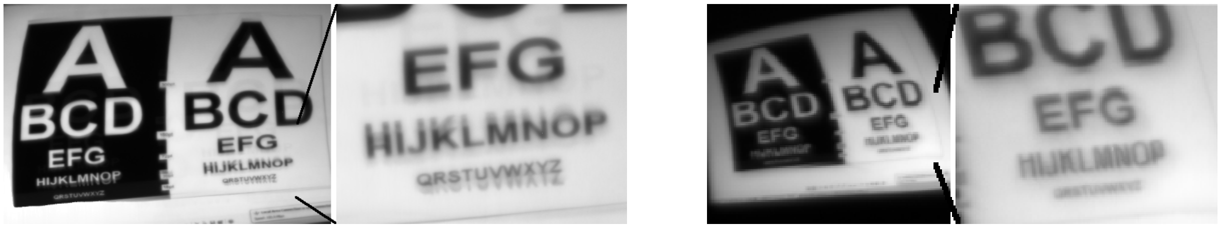

Figure 4. Our results: Reflections in a tea pot from a distance of 10 meters (left) and 30 meters (right), respectively, using the 235 mm Schmidt-Cassegrain telescope and an astronomic camera.

a radius of approximately 7.8 mm. [20], [13]) requires strong magnification to observe the reflections at a long distance. Consequently, the amount of light that can be exploited to observe the reflections is strongly limited, calling for exposure times of several seconds for typical SLR-cameras (both consumer-grade and professional ones) [4]. Second, the human eye is steadily and subconsciously moving, causing a large amount of motion blur, see Figure 1 for illustration. Thirdly, the depth-of-field, i.e., the range of distances at which objects appear sufficiently sharp, is very low when using telescopes, additionally giving out-of-focus blur.

In this section we show how to overcome these problems and remove the blur from the reflections in the user's eye in realistic settings, using image deconvolution algorithms. In Section 2.1 we give some details on the hardware we used, in Section 2.2 we describe the types of blur that occur in our setting, in Section 2.3 we give an introduction to image deconvolution, in Section 2.4 and Section 2.5 we describe two methods that we used to capture the PSF, and in Section 2.6 we sum up the results. Images demonstrating our findings are given in Figure 6.

2.1. Hardware Equipment

In previous work, the long exposure times that are needed to capture the dim reflections from the eye caused a substantial amount of motion blur. By using more light-sensitive equipment we reduced the required exposure time and thus decreased the amount of motion blur.

First, we used a more light-sensitive camera. We have chosen an astronomical camera since these are widely available at reasonable prices and have a quantum efficiency (the percentage of photons that arrive at the camera sensor which are actually counted) close to the theoretical optimum. (Astronomic cameras are additionally optimized for long exposure times, a feature we do not need for taking reflections from the eye, but it will also help us with stationary objects.) Another requirement is the optical resolution. We capture the reflections of a monitor running at 1024 by 768 pixels; the reflection did not fill the entire image, which makes aiming easier. We used a SBIG ST-10XME camera as it combines both properties at a reasonable price (approx. 6000 USD). The camera has a large pixel size of $6.8\ \mu\mathrm{m}$, is monochromatic (no color filters that block light), and has a resolution of 16 bits per pixel. Its quantum efficiency (the percentage of photons that arrive at the camera sensor which is actually counted) reaches 90% for wavelengths around $600\ \mathrm{nm}$ (green/yellow), and is larger than 50% over the whole range of visible light [27].

Second, we used a better telescope, a Celestron C9.25 Schmidt-Cassegrain. The Schmidt-Cassegrain construction is very compact compared to the classical Newton-design (it has a length of $580\ \mathrm{mm}$ and a focal length of 2350 mm), and typically has better image quality (although there are high-quality Newton telescopes as well), but are more expensive than (simple) Newtons. Compared with previous work [4], this telescope offers a slightly larger diameter and better coating, which leads to an additional gain of approximately 20%.

2.2. Out-of-focus Blur and Motion Blur

In any image captured with a large enough aperture, objects that are either closer or farther away than the selected focus distance will be blurred. This *out-of-focus* blur is often quite moderate for medium aperture SLR cameras – and sometimes even desirable in photography as a visual effect. In our application, as a large aperture telescope is applied for improved light efficiency, the blurring can be rather drastic (e.g., see Figure 1), posing a significant obstacle when capturing a high-resolution image of an object at unknown or varying distance such as the slightly moving eye.

The range of distances in which objects appear "sufficiently sharp" for a fixed focus setting is called the *depth of field* (DOF). The notion of "sufficiently sharp" in image processing applications is related to the *circle of confusion*, the area covered by a single object point projected onto the image sensor given the current focus settings. If the circle of confusion is significantly larger than one camera pixel the object will appear blurred. For an optical system consisting of a single lens with focal length f and aperture D, at a given distance s and for a pixel size v, the DOF is given by

$$DOF = \begin{cases} \frac{2HFDs^2}{HFD^2 - s^2} & \text{for } s < HFD \\ \infty & \text{otherwise} \end{cases}$$

where $HFD \approx \frac{f^2}{\frac{f}{D}v}$ is the so-called *hyper-focal distance*, corresponding to the minimal focal distance such that a point at infinity is still sufficiently sharp. For our equipment we have $f = 2350$ mm, $D = 235$ mm, $d \approx 10$ m, and $v = 6.8$ μm. Consequently, the DOF is approximately 2.5 mm, only. Such a small DoF is a major hurdle for taking sharp images, in particular for moving objects, as our experiments show. This hurdle was not present in earlier work, which primarily considered stationary objects that offer sufficient time for setting the focus correctly [4].

Additionally, with the required exposure times of more than one second it is obvious that the object, i.e., the person we spy on and in particular his eye, will not be steady but move, causing a substantial amount of *motion blur*.

Previous work to eliminate motion blur from images (e.g. [31], [24], [35]) are not immediately applicable to our setting, since the strong curvature of the eye leads to additional distortions that are not addressed by prior techniques.

We apply non-blind deconvolution techniques to address the problem of motion and out-of-focus blur [25], [19]. Both motion and out-of-focus have the effect of convolving the desired image with a filter kernel, also called point-spread function (PSF). Once we obtained the correct PSF we can use the techniques from Section 2.3 to invert the effect of the convolution, i.e., obtain a (more or less) sharp image again. We will provide more details on deconvolution in the following.

2.3. Image Deconvolution Primer

Blur can be described by a *point spread function (PSF)* $H(x, y)$ which models the redistribution of energy from each point y of the (unobservable) sharp image to each point x of the blurred image. In many cases, the PSF can be assumed to be *spatially invariant,* i.e., the distribution of energy from different source points is equal up to translation, $H(x, y) \equiv h(y - x)$. The blur process can then be described by a simple convolution with h. Assuming an additive measurement noise n on the blurred image, the observed image f depends on the sharp image g via $f = g{*}h{+}n$.

Due to the ubiquity of blur, its removal – *deblurring* or *deconvolution* – has long been a subject of investigation, and many algorithms have been devised. However, the deconvolution problem is highly ill-posed (i.e., the solution is not necessarily unique, and small perturbations in the input may lead to big perturbations in the output), and no method suits all needs equally well.

A time-proven approach to deconvolution is the *Wiener filter* [33]. It exploits the convolution theorem to restate the problem in the Fourier domain as $\hat{f} = \hat{g} \cdot \hat{h} + \hat{n}$. An approximation to $\hat{g}$ could then be computed by inverse filtering $\hat{u} = \hat{f}/\hat{h}$, which runs into problems at frequencies where $\hat{h}$ is very small. Wiener filtering regularizes the process at exactly these frequencies, yielding

$$\hat{u} = \frac{1}{\hat{h}} \cdot \frac{|\hat{h}|^2}{|\hat{h}|^2 + K^2} \cdot \hat{f} \; . \tag{1}$$

with a parameter $K > 0$. Combined with Fast Fourier Transformation, this is a fast and simple linear filtering procedure that can be proven to be optimal in terms of mean squared error when the noise n is Gaussian. However, as a linear method it is bound to produce the visually unpleasant "ringing" artifacts [6]. Moreover,

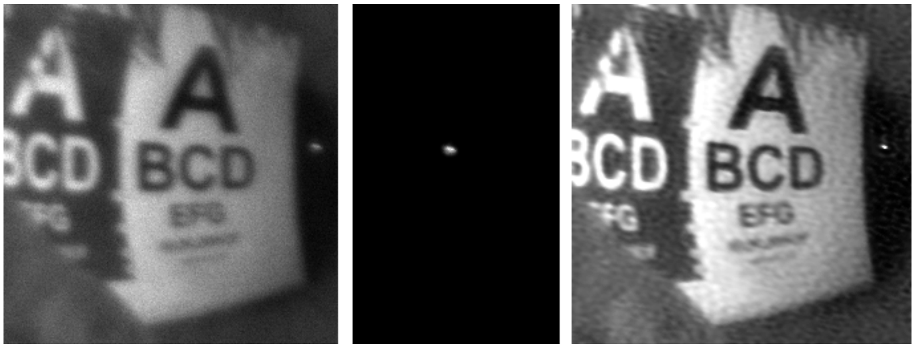

Figure 6. Example of an image (in the eye, from 10 meters) with the PSF captured at the same time (left), the PSF extracted from the small glint to the right of the monitor reflection (middle), and the result of deconvolution (right).

its performance decreases in presence of non-Gaussian noise, and it can hardly handle small imprecisions in PSF estimates, or small violations of spatial invariance.

A widespread alternative is *Richardson-Lucy deconvolution (RL)* [26], [19]. Though computationally more costly than the Wiener filter, RL is still fairly fast. It is a simple nonlinear iteration, one step of which reads

$$u^{k+1} = \left(h^* * \left(\frac{f}{u^k * h} \right) \right) \cdot u^k \tag{2}$$

where h^* denotes the adjoint of the point-spread function, $h^*(x, y) = h(-x, -y)$. This algorithm is better adapted to Poisson noise in the data; in particular, the positivity of grayvalues is a built-in constraint. In absence of noise, the sharp image g would be a fixed point of (2). However, due to the ill-posedness of deconvolution, even small perturbations are amplified over time such that after a while noise begins to dominate the filtered image. As a result, the deconvolution process needs to be regularized by the number of iterations, with less iterations meaning less sharpness, but also less noise. For deblurring the reflections captured in the eye we use this variant of Richardson-Lucy deconvolution.

2.4. Offline-Measurement of the PSF

It turned out that out-of-focus blur can be quite accurately removed from an image, provided that the PSF could be measured accurately. This is the case when the exact location of both the focus plane and the object are known. (This is demonstrated in Figure 9, where the reflection is taken from a static object, so the PSF can be measured accurately.)

For a moving target, however, the exact locations are typically not known. In this section we will show that measuring a series of PSFs for varying distances and trying to deconvolve the blurred image with each of them, followed by manually selecting the best image, yields good results. The main advantage of measuring the PSFs offline is that we can use very long exposure times when capturing the PSF, as this is done under lab conditions, thus obtaining an accurate PSF with low noise, which is crucial for deconvolution algorithms to work well.

Alternatively, more sophisticated methods for determining the PSF exist [35], [11]. However, our experiments show that these have problems when faced with the significant amount of noise that is present in our measurements. Our method has the advantage that it is very robust and tolerates some errors in the measurement. Even dim images can be enhanced significantly.

For the a priori calibration, we use a bright source of light (a white LED) with a circular mask and capture its reflection in a small sphere. Taking its reflection in a sphere greatly decreases the light's apparent size so that it closely resembles a true point light source. We capture several such images under identical conditions and average over them to further decrease the noise level, which is a standard technique in astronomical imaging. A sequence of such measured PSFs for different levels of out-of-focus blur is displayed in Figure 7. The circular shape of the measured PSFs is slightly irregular due to slight imperfections of the telescope.

Once we obtained a sufficiently large sequence of measured PSFs, given an unsharp image, we run the deconvolution algorithm with each of these measured PSFs as input. Finally, we select the output image that gives the best results, based on their apparent sharpness.

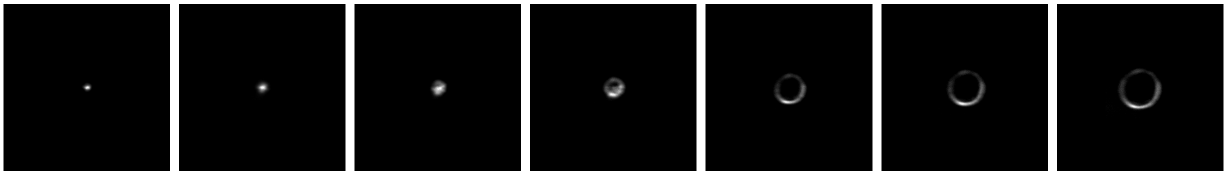

Figure 7. A sequence of measured PSFs, after stacking and post-processing. Their circular shape coined the notion of “circles of confusion” in astronomic imaging.

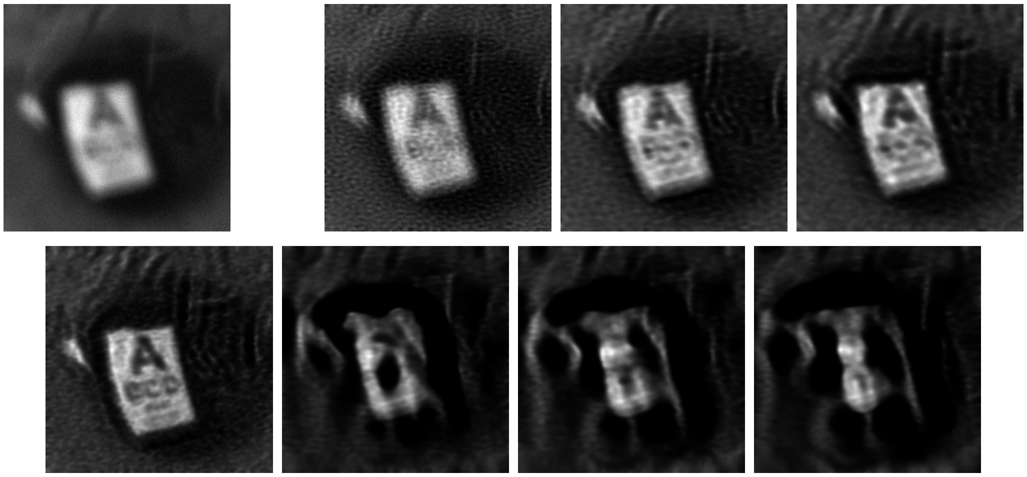

Figure 8. Example of an unsharp image with unknown PSF (first image), and the results from deconvolution using the series of PSFs from Figure 7. The fourth PSF yields the best result.

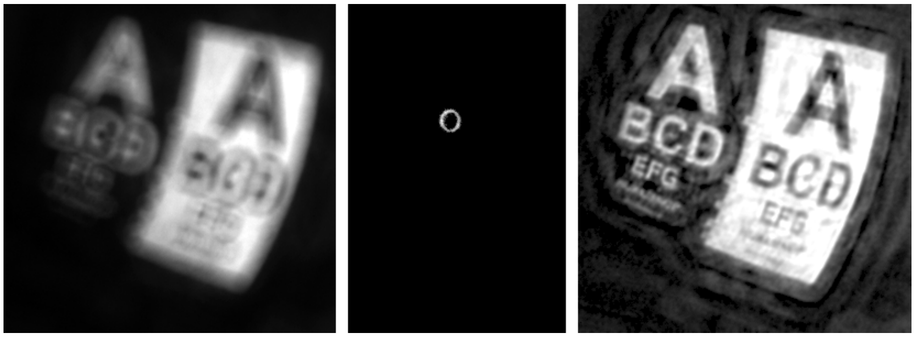

Figure 9. Removing out-of-focus blur with deconvolution: Blurred image (left), the measured PSF (middle), and the result of deconvolution (right). These images were taken from a stationary object, the correct PSF was measured.

2.5. Online-Measurement of the PSF

Next, we describe an alternative method that allows for precisely determining the PSF that was effective in a particular measurement. In addition to accurately dealing with out-of focus blur, this technique also measures any motion blur that occurs while capturing the image.

Basically, the technique relies on having a single bright point with a dark surrounding area close to the monitor; the image of this single point on the sensor then constitutes the PSF. The crucial part for this approach is the selection of the light source: if the source is not bright enough, the measurement will be too noisy; if the source is too large (such as electric bulbs), the measurement will be inaccurate. Suitable light sources turned out to be either a laser or a bright LED.

For a realistic attack, invisible light, e.g. infrared light, is preferable as it has the advantage that it facil-

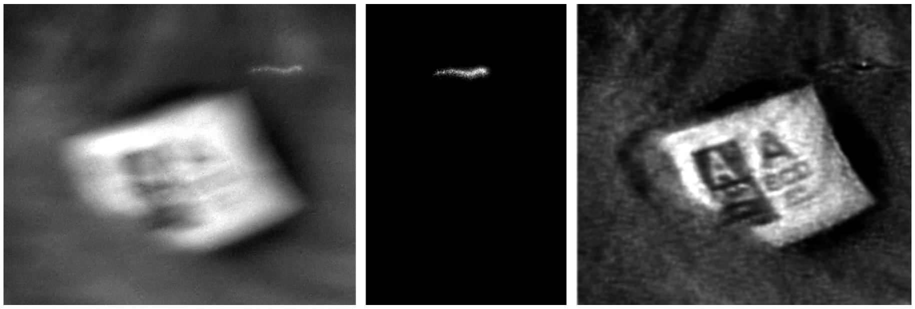

Figure 10. Example of an extremely blurred image (in the eye, from 10 meters) with PSF captured at the same time (left), the extracted PSF (middle), and the result of deconvolution (right).

itates the task of separating the PSF from background light, and it additionally does not capture the attention and hence the suspicion of the observed user. The light source can be mounted at any position that ensures that the reflection of the light source in the eye of the user is captured by the telescope. At the telescope, the captured image passes a selective mirror that reflects visible light while letting infrared light pass. After additional filtering both light paths can be captured as usual. (Some care has to be taken to remove potential effects from different chromatic aberrations caused by the different wavelengths, and possibly different sensor characteristics.) Measuring the PSF in this way should yield very accurate results. However, the use of bright invisible light sources is prohibitively dangerous for academic purposes. We hence did not implement it and used visible light instead, while the overall approach did not change. We believe that both approaches should give comparable results.

2.6. Discussion of Results

Results with the PSF measured offline are shown in Figure 8. We obtained a sufficiently large number of measured PSFs, then ran the deconvolution algorithm with each of these measured PSFs. Finally, we select the output image that gives the best results.

This approach works very well if there is no motion blur present in the captured image, thus it is very useful when spying on stationary objects. The advantage of this method is that the PSF can be accurately measured offline, since one can use long exposures times to reduce the noise level and to increase the image quality. However, if there is some amount of motion blur present in the captured image, this approach performs rather poorly.

In the situations commonly encountered with the human eye, the second approach performs much better. Two blurred images are shown in Figure 6 and 10 on the respective left sides. The overall setup is identical to using invisible light and it should yield comparable results, except that using visible light would capture the attention of the user and would hence render the attack less feasible in realistic settings.

The PSF was extracted from the images as shown in the respective middle pictures. The result after deconvolution (200 iterations, running times of approximately 1 minute on an ordinary desktop machine). We also tested the Wiener filter, which runs faster but results are slightly worse.

There are some possible improvements and variations that we identified: Other sources of light that can be used to measure the PSF. For example Status LEDs of the monitor or of any other devices might be usable. Colored LEDs constitute a particularly promising candidate because their typically narrow spectrum is well-suited for a matching filter to yield a good contrast. Even stationary light sources such as lights at a nearby parking lot might be suitable. While the use of deconvolution techniques has significantly contributed to removing out-of-focus blur, accurately focusing on moving objects still is a major challenge. A conveniently usable, precise *auto-focuser*, a feature that is available in almost any modern camera, would be a great help. However, designing an auto-focuser that can handle a very narrow depth-of-field and moving objects, and has the accuracy that is needed for successfully recovering information from captured reflections is a non-trivial task. A larger image sensor – or a sensor with higher resolution – would facilitate the task of aiming at the user's eye.

3. Diffuse Reflections

In the previous sections we have shown that specular and glossy surfaces like an eye reflect a more or less clear picture of the information on a near-by screen. In this section we will investigate another type of

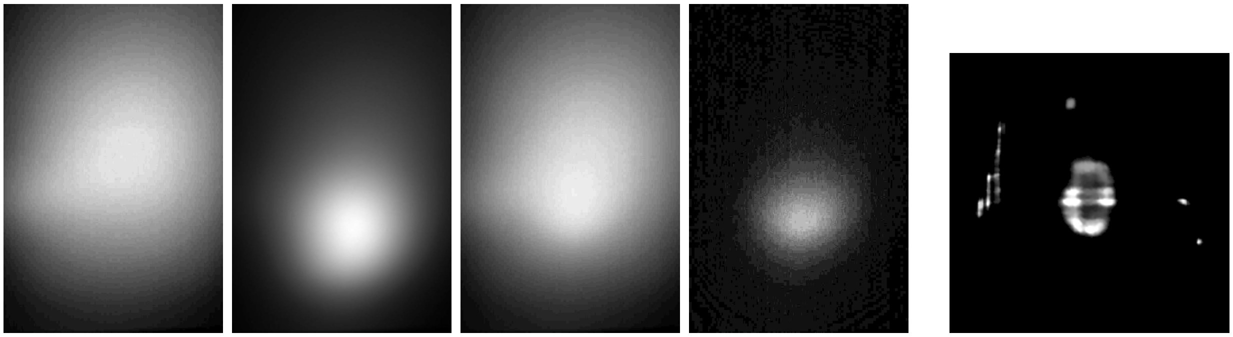

Figure 11. These images show, from left to right, the reflections caused by the black background **(1)**, the letter “C” **(2)**, a small 50x50 pixel white block (the “PSF”) **(3)**, the difference between (3) and (1), i.e., the actual PSF **(4)**, and the result of deconvolution of (2) subtracted (1), i.e., the letter “C” **(5)**. The luminosity of these images was scaled individually to increase readability, and (5) is not to scale.

attack: we investigate to what extend one can spy on reflections on diffuse surfaces.

A diffuse surface will be lit up homogeneously according to the total emitted light of the screen as the reflection of each surface point integrates over all directions, i.e. over all pixels on the screen. In this typical setup, the spatial variation on a diffuse surfaces caused by a near-by screen will therefore be too smooth to be informative. However, a clear picture will be formed if a sharp, spatially varying pattern is projected onto the diffuse surface, e.g. the standard case of a video projector.

Using a privacy filter on a monitor will limit the range of directions into which a monitor emits light, so an observer looking at the screen from a shallow angle might observe a dark screen. Depending on the width of the emitted cone, the screen with the privacy filter will act as an unfocused projector and shape a spatially varying pattern on a near-by diffuse surface, forming a blurred image.

In this section we will show that applying deconvolution, a coarse structure of the displayed image will become visible. This is demonstrated in Section 3.2. However, the resolution is limited as the emitted cones are typically still too wide to reconstruct a sharp image, due to largely overlapping filter kernels per pixel. we will show how to effectively limit the obtainable resolution for a certain setting in Section 3.3.

3.1. Advanced Image Deconvolution

The PSFs we have to deal with when spying on reflections in diffuse surfaces are much larger, thus better deconvolution algorithm are required. In this section we describe a recently proposed variant of Richardson-Lucy deconvolution that is more robust, called *robust and regularized Richardson-Lucy deconvolution (RRRL)*. While RRRL achieves a higher reconstruction quality than standard RL, its computational cost is significantly higher. We reserve its use therefore mainly to those cases where standard RL gives no reasonable results at all. This applies particularly to the case of diffuse reflections.

To improve the reconstruction of image structures in RL, an additional regularization was introduced by Dey et al. [9]. It is derived from total variation (TV) regularization [21] which plays an important role in contemporary image processing. In contrast to the regularization by iteration count, its activity at different image locations adapts to image structures, thereby allowing a better preservation of structures (like edges) in the deconvolution process.

Another strategy that has proven successful in improving image processing algorithms is robustification, see e.g. [36] for an application in deconvolution. In methods that correct errors in an iterative fashion robustification is done by applying a weighting function with values smaller than one that gives large errors a reduced weight in the correction step. In this way, the process gains robustness against outliers, and is better capable of handling strong noise. Even imprecisions in PSF estimation can be coped with, and also moderate violations of model assumptions such as spatially invariance of blur, or the loss of information by blurring across image boundaries.

Using a regularization similar to [9] together with a robustification, we obtain the iteration formula

$$u^{k+1} = \frac{h^* * \left(\varphi(r_f(u*h))\,\frac{f}{u^k*h}\right) + \alpha\left[\operatorname{div}\left(\psi(|\nabla u^k|^2)\,\nabla u^k\right)\right]_+}{h^* * \varphi(r_f(u^k*h)) - \alpha[\operatorname{div}\left(\psi(|\nabla u^k|^2)\,\nabla u^k\right)]_-}\,u^k\,, \tag{3}$$

which we will call robust and regularized Richardson-

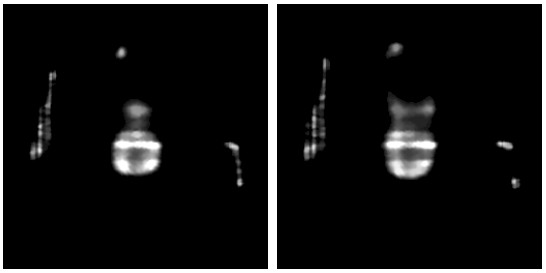

Figure 12. Two more examples for deconvolution: The letters “A” (left) and “B” (right).

Lucy deconvolution (RRRL). Here we use the abbreviation $[z]_\pm := \frac{1}{2}(z \pm |z|)$, and φ, ψ denote monotonically decreasing nonnegative functions on the nonnegative real numbers. In our experiments, we use $\varphi(z) := (z^2 + \varepsilon)^{-0.1}$ and $\psi(z) := (z^2 + \varepsilon)^{-0.5}$ with a small positive ε. The asymmetric penalizer function $r_f(w) = w - f - f \ln(w/f)$ is used to measure the reconstruction error in step k, i.e., the deviation of $u^k * h$ from f. The weight parameter α controls the influence of TV regularization. More details on RRRL can be found in the preprint [2] by one of the authors, which is in preparation.

3.2. Results

Figure 11 shows the results of deconvolution of a diffuse reflection. The setup was as follows. We placed the monitor (with the privacy filter) against a white wall, at a distance of 25 cm (this is the depth of the keyboard, thus it essentially provides a lower bound) and captured the diffuse reflection with a digital camera. The monitor showed a single letter, white on black background, with an unrealistically large size of 10 cm. (The camera used was a Canon EOS 400d, exposure time was 10 sec at F 5.6 and ISO 100. Captured as RAW, and exported with *linear* scaling of the intensity values.) It turned out that the black pixels of the monitor still leak a substantial amount of light. This leakage seems to be directed differently than the white pixels, so it would disturb the normal deconvolution. For that reason we subtracted this light by capturing an additional image of the reflections for a completely black monitor image, and we subtracted this image from all other images. The result was scaled down, slightly cropped and completed to a size of 256×256 pixels. The PSF was captured in a similar manner.

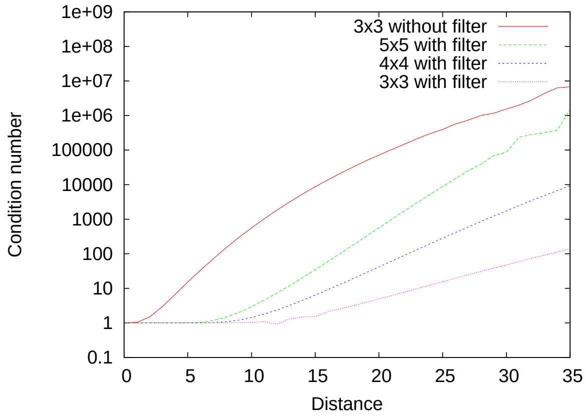

Figure 13. Condition numbers for varying distances and several setups: For a letter of 10 cm height, the matrix for obtaining a resolution as given, with or without privacy filter as indicated. In image deconvolution, condition numbers above 100 are considered hard, and condition numbers above 10^5 are certainly out of reach.

On this image we applied robust and regularized Richardson-Lucy deconvolution as described above, some results are shown in Figure 11. Deconvolution ran for 10’000 iterations in 15 minutes on a single workstation. Finally, we re-scaled, gray-scaled and flipped the image horizontally, so the letters are in the correct orientation.

3.3. Limitations

Next, we will give a theoretical bound on the applicability of this type of attacks, and we will see that our results were essentially optimal.

The light transport from a monitor image L to the image E formed on the diffuse reflector (both seen as vectors) can be expressed as the light transport matrix M:

$$E = ML. \tag{4}$$

To compute M we have simulated the light transport. In the case without the privacy filter we roughly estimated the distribution to follow the function $\cos^4 \theta$ where θ is the angle between the viewing direction and the monitor normal. With the privacy filter in place the emitted light is much more directed, i.e. concentrated around the normal, resulting in a distribution following $cos^{93.4}\theta$, in our case.

In order to reconstruct the monitor image L from the captured reflection E, i.e., to perform the deconvolution, the transport matrix M needs to be inverted: $L = M^{-1}E$. In Figure 13 we plotted the condition number, i.e. the ratio of the maximal to minimal singular value of M ($\kappa(M) = \frac{\|M^{-1}\|}{\|M\|}$), that is correlated

	Costs	Security	Robustness	Comfort
No reflecting objects	+	o	-	-
Window blinds	+	+	o	o
No place to hide	o	o	o	+
Polarization	-	o	o	+
Notch filters	-	+	+	+

Table 1. Evaluation of several countermeasures.

to the stability of the inversion process, for different pixel configuration and distances of the two planes. It is read as follows: At a distance of $25\ \mathrm{cm}$ one should be able still resolve a 3×3 pixel pattern on a patch of size $10\ \mathrm{cm} \times 10\ \mathrm{cm}$, while the condition number for a resolution of 4×4 is borderline, and resolving 5×5 pixels definitely exceeds numerical stability. In the case of a monitor without a privacy screen no reconstruction should be possible if the reflector is more than $6\ \mathrm{cm}$ away from the scene. These simulated numbers nicely correlate with our real experiments presented in Section 3.2: While simple letters such as a “C” still are readable when shown with a resolution of 3×3 pixels, more complex letters such as the “A” and “B” are hardly readable with a resolution of 4×4 pixels.

4. Countermeasures

In this section we discuss how the two attacks – eye reflections and reflections on diffuse surfaces – can be prevented. Some simple countermeasures immediately come to mind. *Avoiding all reflecting objects* certainly provides some level of security. The main problem with this approach is that the number of possibly dangerous objects is vast, and that even eye-glasses and the human eye can pose a threat. However, avoiding as many objects as possible makes the attack harder to carry out, and it should be sufficient to provide a medium level of security. Using *window blinds* counters the attack in many cases, however, having the windows always covered completely is not overly practical. Blinds may be partially opened accidentally or by a person not aware of the threat.

In [4] it was already described that *Rayleigh’s Criterion* states a lower bound on the diameter of the telescope which is necessary to obtain sharp images from a given distance. Avoiding any suitable hiding places for an adversary within these bounds thus constitutes a viable countermeasure. This approach offers a reasonable level of security for those cases where the building grounds can be easily controlled, however, it performs badly if there are other buildings in proximity. However, although quite unlikely, it might be possible to build an array of several small telescopes that yields better optical resolution than a single one, or technological advances also may allow to build more compact telescopes that offer resolution beyond the Raleigh bound (so-called “super-lenses” using materials with “negative refraction index” [22], [10]). Additionally, one has to keep in mind that Rayleigh’s Criterion is not necessarily a strict bound. Given some knowledge about the scene, in our case images of text, it is possible to use deconvolution algorithms to improve even on this bound ([30], page 2).

In the following we present some more advanced countermeasures that offer better security, at higher costs.

4.1. Polarization

It is a well-known optical phenomenon that two (linear) polarization filters aligned at 90 degrees will block all light, but a single filter will let pass 50% of (previously unpolarized) light. Putting one filter on the monitor and a rotated filter on the window, the user can still read the monitor with slightly reduced brightness, but an attacker outside the window can not. This was proposed, in [23] as a measure to protect privacy. Today this is even easier to implement, as modern LCD monitors already do have a polarization filter equipped by their construction.

Unfortunately, this approach does not work well in practice, as is shown in Figure 14: While two aligned filters should block 100% of the light, by means of imperfect alignment, which is inevitable in a practical environment, or imperfect filter characteristics, its effectiveness will be slightly lower. Using longer exposure times, the monitor image can be recovered. Furthermore, metallic surfaces change the polarization of light, rendering the filters ineffective.

4.2. Notch-Filter

Another possible countermeasure is based on optical notch-filters, optical filters that block a very narrow band of wavelengths and let pass all other wavelengths (see Figure 15). The optical spectrum emitted by TFT monitors is mainly determined by the characteristics of the background light. Colored LEDs typically have a very narrow spectrum. Some specialized recent monitors, e.g. the ACER AL1917L, use LEDs as background light, and thus do have a very characteristic spectrum. The measured spectrum for a fully white monitor image is shown in Figure 16. While the manufacturers purpose is to increase the color-characteristics of the monitor, we can exploit this

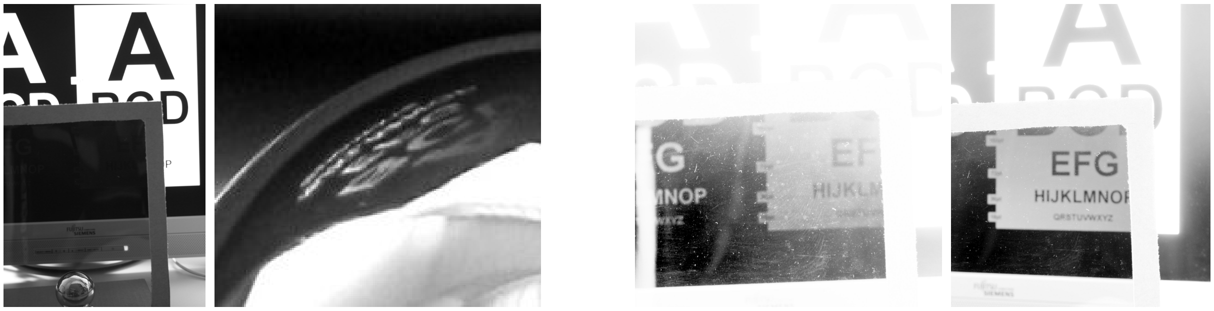

Figure 14. These images show that the protection offered by suitably aligned polarization filters is far from being perfect. While blocking most light (first image), metallic objects change polarization of light, making the monitor content readable (second image, magnification from first image). Increased exposure times still reveal the monitor contents (third image), in particular if the alignment of the two polarization filters is not perfect (fourth image).

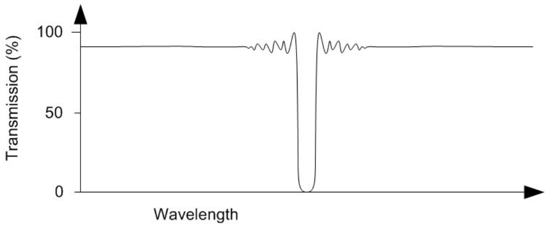

Figure 15. Schematic transmission characteristics of optical notch filters.

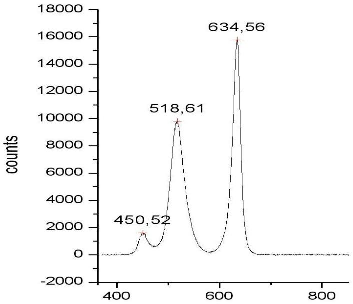

Figure 16. Spectrum measured from a commercially available ACER AL1917L monitor with LED background light.

for our purposes. By designing very narrow optical notch filters designed to match these frequency bands it would be possible to suppress exactly the monitor image, while for images that are created by continuous spectra such as emitted by sunlight or light-bulbs, the image quality is hardly influenced.

When trying to implement this countermeasure we faced a practical problem. Commercially available optical notch filters do not match our specific needs (they are typically designed for optical experiments, thus very high quality and expensive, and for specific center frequencies only), and the custom design of these filters in small quantities is prohibitively expensive. However, for the red band emitted by the monitor, with the peak at 634.56 nm, there is a commercially available filter which is almost suitable, with a peak at the laser-line 632.6 nm (HeNe-laser). Our model has a width of 31.6 nm, which is slightly too narrow. Still, measurements show that it block 88% of the red light emitted by the monitor, while barely affecting "normal" light. Figure 17 shows the filter in front of red text (left image), and in front of an apple lightened by an ordinary energy-saving light bulb, which has a (partly) continuous spectrum (right image). An additional advantage of this measure is that this also protects against diffuse reflections and reflections in metallic objects.

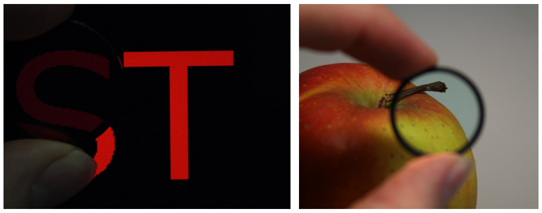

Figure 17. These images show the protection offered by an off-the-shelf optical notch filter.

5. Conclusion

Prior to our work, compromising reflections could only be exploited in the presence of stationary, reflecting objects such as tea pots, glasses, or spoons. Removing these objects from the work place rendered the attack impossible.

We explored several possibilities to spy on confidential data in the absence of these objects and evaluated appropriate countermeasures. First, we demonstrated that reflections in the user's eye can be successfully spied on using image deconvolution algorithms. At the same time these results improve our ability to spy on stationary objects. Second, we explored to what extent diffuse reflections can be used to reconstruct the original image, and were able to give bounds stating that in all interesting cases such an attack will not reveal more than basic shapes. Third, we evaluated several possible countermeasures. Compared with previous work, our improvements led to roughly a four times better resolution for a given telescope diameter than previous work.

References

[1] R. J. Anderson and M. G. Kuhn. Soft tempest – An opportunity for NATO. In *Information Systems Technology (IST) Symposium "Protecting NATO Information Systems in the 21st Century"*, 1999.

[2] Anonymous author. Variational approaches to positivity-constrained image deconvolution. Technical report, Anonymous institution, 2008. In preparation.

[3] D. Asonov and R. Agrawal. Keyboard acoustic emanations. In *Proc. of the 2004 IEEE Symposium on Security and Privacy*, 2004.

[4] M. Backes, M. Dürmuth, and D. Unruh. Compromising reflections – or – How to read LCD monitors around the corner. In *Proc. of the 2008 IEEE Symposium on Security and Privacy*, 2008.

[5] R. Berry and J. Burnell. *The Handbook of Astronomical Image Processing*. Willmann-Bell, 2 edition, 2005.

[6] M. Bertero and P. Boccacci. *Introduction to Inverse Problems in Imaging*. IoP Publishing, Bristol, 1998.

[7] R. Briol. Emanation: How to keep your data confidential. In *Symposium on Electromagnetic Security for Information Protection*, 1991.

[8] P. V. Cittert. Zum Einfluß der Spaltbreite auf die Intensitätsverteilung in Spektrallinien II. *Zeitschrift für Physik*, 69:298–308, 1931.

[9] N. Dey, L. Blanc-Feraud, C. Zimmer, Z. Kam, J.-C. Olivo-Marin, and J. Zerubia. A deconvolution method for confocal microscopy with total variation regularization. In *Proc. 2004 IEEE International Symposium on Biomedical Imaging: Nano to Macro*, volume 2, pages 1223–1226, Sophia Antipolis, France, April 2004.

[10] N. Fang, H. Lee, C. Sun, and X. Zhang. Sub-diffraction-limited optical imaging with a silver superlens. *Science*, 308(5721):534 – 537, April 2005.

[11] R. Fergus, B. Singh, A. Hertzmann, S. T. Roweis, and W. T. Freeman. Removing camera shake from a single photograph. *ACM Trans. Graph.*, 25(3):787–794, 2006.

[12] H. J. Highland. Electromagnetic radiation revisited. *Comput. Secur.*, 5(2):85–93, 1986.

[13] P. Kaufman and A. Alm, editors. *Adler's Physiology of the Eye: Clinical Application*. Mosby, 10 edition, 2003.

[14] M. G. Kuhn. Optical time-domain eavesdropping risks of CRT displays. In *Proc. of the 2002 IEEE Symposium on Security and Privacy*, 2002.

[15] M. G. Kuhn. *Compromising Emanations: Eavesdropping Risks of Computer Displays*. PhD thesis, University of Cambridge, 2003.

[16] M. G. Kuhn. Electromagnetic eavesdropping risks of flat-panel displays. In *Proc. of the 4th Workshop on Privacy Enhancing Technologies*, pages 88–107, 2005.

[17] M. G. Kuhn. Security limits for compromising emanations. In *Proc. of CHES 2005*, volume 3659 of *LNCS*. Springer, 2005.

[18] J. Loughry and D. A. Umphress. Information leakage from optical emanation. *ACM Transactions on Information and Systems Security*, 5(3):262–289, 2002.

[19] L. B. Lucy. An iterative technique for the rectification of observed distributions. *The Astronomical Journal*, 79(6):745–754, June 1974.

[20] K. Nishino and S. K. Nayar. Corneal imaging system: Environment from eyes. *International Journal on Computer Vision*, 2006.

[21] S. Osher and L. Rudin. Total variation based image restoration with free local constraints. In *Proc. 1994 IEEE International Conference on Image Processing*, pages 31–35, Austin, Texas, 1994.

[22] J. B. Pendry. Negative refraction makes a perfect lens. *Phys. Rev. Lett.*, 85(18):3966–3969, Oct 2000.

[23] Qwest Communications Int'l Inc. (Denver, CO): Polarizing privacy system for use with a visual display terminal. United States Patent 6262843, Filed 12/31/1997, online at http://www.freepatentsonline.com/6262843.html.

[24] R. Raskar, A. Agrawal, and J. Tumblin. Coded exposure photography: Motion deblurring using fluttered shutter. *ACM Trans. Graph.*, 25(3):795–804, 2006.

[25] W. Richardson. Bayesian-based iterative method of image restoration. *J. Opt. Soc. Am.*, 62(1):55, 1972.

[26] W. H. Richardson. Bayesian-based iterative method of image restoration. *Journal of the Optical Society of America*, 62(1):55–59, 1972.

[27] Santa Barbara Instrument Group. The SBIG ST-10XME CCD camera. Online at http://www.sbig.com/sbwhtmls/online.htm.

[28] A. Shamir and E. Tromer. Acoustic cryptanalysis – On nosy people and noisy machines. Online at http://people.csail.mit.edu/tromer/acoustic/.

[29] P. Smulders. The threat of information theft by reception of electromagnetic radiation from RS-232 cables. *Computers & Security*, 9:53–58, 1990.

[30] J. Starck, E. Pantin, and F. Murtagh. Deconvolution in astronomy: A review. *Publications of the Astronomical Society of the Pacific*, 114:1051–1069, 2002.

[31] J. Telleen, A. Sullivan, J. Yee, P. Gunawardane, O. Wang, I. Collins, and J. Davis. Synthetic shutter speed imaging. In *Eurographics 2007*, 2007.

[32] W. van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4:269–286, 1985.

[33] N. Wiener. *Extrapolation, Interpolation and Smoothing of Stationary Time Series with Engineering Applications*. MIT Press, Cambridge, MA, 1949.

[34] J. Young. How old is tempest? Online response collection. Online at http://cryptome.org/tempest-old.htm, February 2000.

[35] L. Yuan, J. Sun, L. Quan, and H.-Y. Shum. Image deblurring with blurred/noisy image pairs. In *ACM SIGGRAPH 2007 papers*, 2007.

[36] M. E. Zervakis, A. K. Katsaggelos, and T. M. Kwon. A class of robust entropic functionals for image restoration. *IEEE Transactions on Image Processing*, 4(6):752–773, June 1995.

[37] L. Zhuang, F. Zhou, and J.D.Tygar. Keyboard acoustic emanations revisited. In *Proc. of the 12th ACM Conference on Computer and Communications Security*, 2005.