Preventing Camera Recording by Designing a Capture-Resistant Environment

Authors

…
…
…
Author emails

Abstract. With the ubiquity of camera phones, it is now possible to capture digital still and moving images anywhere, raising a legitimate concern for many organizations and individuals. Although legal and social boundaries can curb the capture of sensitive information, it sometimes is neither practical nor desirable to follow the option of confiscating the capture device from an individual. We present the design and proof of concept implementation of a capture-resistant environment that prevents the recording of still and moving images without requiring any cooperation on the part of the capturing device or its operator. Our solution involves a simple tracking system that uses computer vision for locating any number of retro-reflective CCD or CMOS camera sensors in a protected area. A pulsing light is then directed at the lens, distorting any imagery the camera records. Although the directed light interferes with the camera's operation, it can be designed to minimally impact the view of other humans in the environment.

1 Introduction and Motivation

By the last quarter of 2004, about 75% percent of mobile phones in Japan were camera phones; it is expected this number will saturate at around 75%-85% in 2005.[1] By 2006, more than 80 percent of mobile phones shipped in the United States and Western Europe will have cameras.[2] Camera phones, and related consumer technologies, make it easy to capture still and moving images anywhere, creating a legitimate concern among those who wish to retain some level of privacy or secrecy. Companies concerned that camera phones compromise the security of their intellectual property often ban such devices from their facilities. These confiscation practices, however, are not always desirable or practical. Although some legal controls and social boundaries may curb inappropriate capture behaviors [2, 3, 8], we want to explore technological opportunities to safeguard against undesired recording without requiring confiscation by an authority or cooperation by the public at large.

---

1 Source: Eurotechnology, Japan K.K., Camera phones: disruptive innovation for imaging, Market and trend report, 5th Version of October 11, 2004

2 Source: Gartner Inc. http://www3.gartner.com/press_releases/pr3mar2004a.html

There has been previous work that addressed this challenge by disabling recording features in the cameras [5, 6, 9]. In this paper, we present an alternative that does not require instrumentation or control of the recording device. Instead, we present a technique for safeguarding the environment itself against recording, creating a so-called "capture-resistant" environment. Our system detects cameras in the environment and emits a strong localized light beam at each device to neutralize it from capturing. Although our approach does have limitations, its main strength is that it requires no cooperation on the part of the camera or its owner and it minimally disturbs the natural viewing experience by the human eye.

2 Related Work

Technical solutions have been proposed to prevent or react to undesired camera capture. Most of these solutions require some sort of instrumentation of a capture device. For example, solutions, such as Safe Haven, leverage the short-range wireless capability available on camera phones (such as Bluetooth or WiFi) to allow the environment to notify the device that the space does not allow photography or other forms of recording [5, 6, 9]. There are many drawbacks to this solution. First, it assumes that the users of the camera would install and use special software on the device and that she would abide by the environmental constraints. Hewlett-Packard has proposed a *paparazzi-proof* camera [7] that automatically modifies images when it receives commands from a remote device. This camera includes a facial recognition feature that selectively blurs certain parts of an image. Other approaches also require different forms of cooperation on the part of the camera or its operator. The Cloak system addresses privacy concerns with surveillance cameras by having users carry a "privacy enabling device" (PED) [1]. This device informs the environment that any footage of the carrier of this device must be sanitized at a later time. A solution called "Eagle Eye" couples a light sensor to a flash unit [4]. When a flash of light is detected, this device instantaneously flashes back. It is small, made to be worn, and obscures a portion of the photographic image, similar to the approach described in this paper. However, it only works against still, flash photography.

We take a significantly different approach from these previous solutions in the design of our capture-resistant environment. First, rather than requiring users to trust cameras to sanitize images after the recording has occurred, we actively impede recording at the point of capture, as with Eagle Eye. Second, unlike many previous solutions, our system does not rely on any cooperation or instrumentation on the part of the capture devices or the people operating them. Our solution addresses video capture, as well as still imagery.

We initially focused on being able to protect stationary regions of an environment, such as a wall. Surfaces in an environment can be covered to prevent capture, but then the surfaces would not be visible. There are numerous commercially-available retro-reflective sprays and shields that can also be placed over a surface to reflect light and flashes in a manner that prevents recording. These solutions create glare that impacts visibility from the human eye as well as the camera sensor. Our solution will minimally impact what an observer in the environment sees while still preventing a camera from being able to record.

3 Design Goals for a Capture-Resistant Environment

Our primary goal in addressing this problem was to design an environment that prevents certain portions of that space from being captured with a standard CCD or CMOS camera.[3] This motivation, and review of past related work, highlights the major design goals for building a capture-resistant environment. These are:

- no need for cooperation or control of the recording devices before, during or after capture;
- prevent the capture of both still images and video; and
- the view of the environment by the naked human eye is minimally impacted.

In addition, this approach should allow for two interesting improvements:

- allow authorized cameras to record; and
- allow mobile entities, such as a person, to be made similarly capture-resistant.

Our design uses a combination of computer vision and projection, described in the next section, to actively search for cameras and systematically block them from recording clear pictures, as opposed to relying on removal or alteration of content later. We envision uses of our system for situations, such as conferences, tradeshows and museums. For example, some museums want to prevent people taking pictures of artwork. Similarly, research laboratories and exhibits at tradeshows want to limit capture of early prototypes and design.

4 A Capture-Resistant Environment

In this section, we present our capture-resistant environment, which consists of two components. The first component, the camera detector, actively tracks CCD sensors in the environment. When the system detects a camera's CCD sensor, the second system component, the camera neutralizer, directs a localized beam of light at each camera's lens to obstruct its view of the scene. This component locates and allows permitted devices to record. For each component, we describe the theory of operation and our proof of concept implementation. We then critically evaluate the limitations of our proof of concept prototype, distinguishing the theoretical limits from the current engineering limitations of our specific implementation and discuss how we can extend our system.

---

[3] CCD and CMOS cameras both use semi-conductor based sensors. Our approach works against both types. We will refer to this category of cameras as "CCD cameras" throughout the rest of the paper.

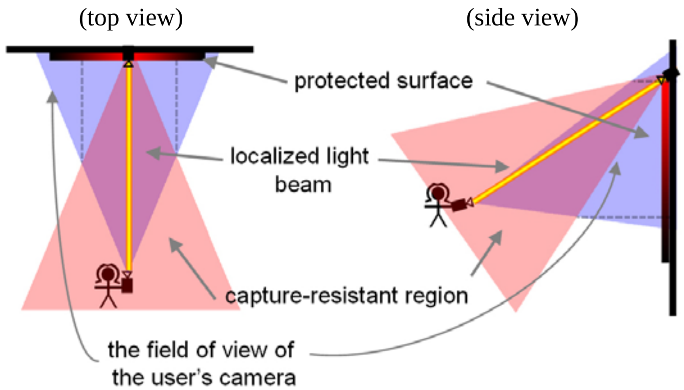


Figure 1. System diagram. When a user introduces a camera into the capture-resistant environment, a camera detector component locates the device within its field of view and the camera neutralizer component emits a localized light beam (yellow) at the camera to block the camera's view of a portion of the surface the system attempts to guard from capture. The red bar indicates the protected surface. The blue indicates the field of view of the user's camera. The pink indicates the camera neutralizer's field of influence. Dashed lines indicate the portion of the protected surface that is affected by the neutralizer's light beam.

4.1 Detecting Cameras in the Environment

CCD cameras have an optical property that produces well-defined light reflections. By tracking these reflections, we can effectively locate and track cameras in an environment.

4.1.1 Theory of Operation

Our camera detector leverages the retro-reflective property of the CCD sensor found on most consumer-level digital cameras. Retro-reflection causes light to reflect directly back to its source, independent of its incident angle. This effect is often noticed on photographs when the camera flash can make a subject's eyes appear to glow red, caused by the retro-reflective property of the retina at the back of the eye. Commercial applications of retro-reflection include traffic signs and reflective clothes commonly worn by road construction workers.

CCD sensors are mounted at the focal plane of the camera's optical lens, making them very effective retro-reflectors. Although there are many objects in the environment that exhibit this property, they are typically imperfect retro-reflectors and can be distinguished from CCD cameras as we demonstrate later. By tracking these retro-reflections we can detect and track cameras pointed at a given area.

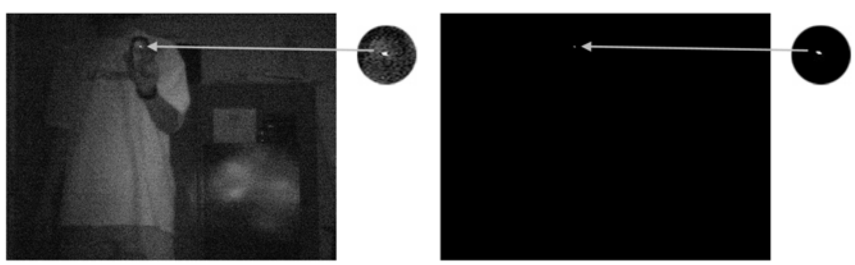
4.1.2 Implementation

To detect cameras in the environment, we use a Sony Digital HandyCam video camera placed in *NightShot* mode. We arranged IR transmitters around the lens and covered the detector's lens with a narrow bandpass IR filter (Figure 3a). This instrumentation, which we will call the detector below, projects an IR light beam outwards from the camera and detects any retro-reflective surfaces within the field of view. We intentionally place the IR illuminator around the perimeter of the detector's lens to ensure a bright retro-reflection from cameras within the field of view of the detector and pointed directly at it or tilted away at slight angles (which we computed to be up to roughly ±20°). This retro-reflection appears as a bright white circular speckle through the IR filtered camera (Figure 2).

We detect reflections by simply locating bright regions in the camera view above a certain luminance threshold (Figure 2). Because we employ a thresholding technique, there is no limit to the number of the cameras that can be detected within the cross-section of the camera detector. In the next section, we will discuss how to handle false positives and false negatives.

Our system effectively tracks cameras at a rate of 15 Hz. A more powerful computer could track at 30 Hz, however 15 Hz is sufficient because a user must hold the average camera still for at least this period of time to avoid motion blur in her picture.

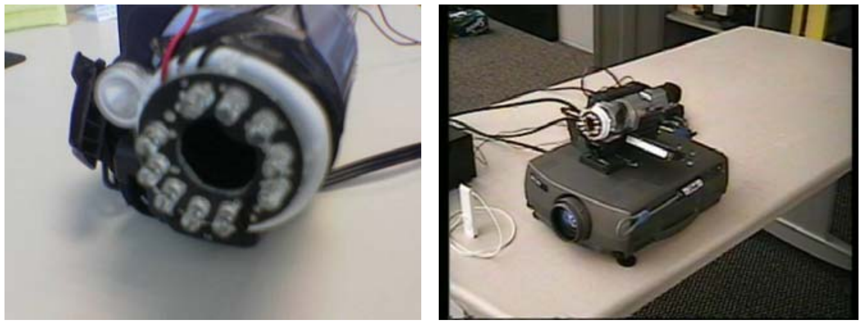
The camera detector has about a 45° field of view. We found that reflections from cameras of varying shapes and sizes can be detected up to 10 meters away. In our proof of concept, at 5 meters away, the cross-section of the detector camera's field of view is roughly a 4m width x 3m height area. Although a zoom lens can be added to a camera, we estimate that 5 meters is roughly the length of a reasonably-sized room. Room sizes and walls naturally prevent people from recording our capture-resistant environment from afar. Our current proof of concept only involves a single detector unit. To ensure that we can detect cameras from all angles, we can measure the angle at which users can approach the surface. Accordingly, we can determine how many detector units we must use to cover that range. We can add additional detectors



(a) (b)

Figure 2. On the left, an unprocessed IR view captured by our camera detector with plenty of ambient light in the room. A person holds a camera phone pointed at a region in the environment we want to protect from capture. On the right is the processed view. The camera is detected by locating a bright white circular speckle.

throughout the environment to find cameras from farther away if needed.

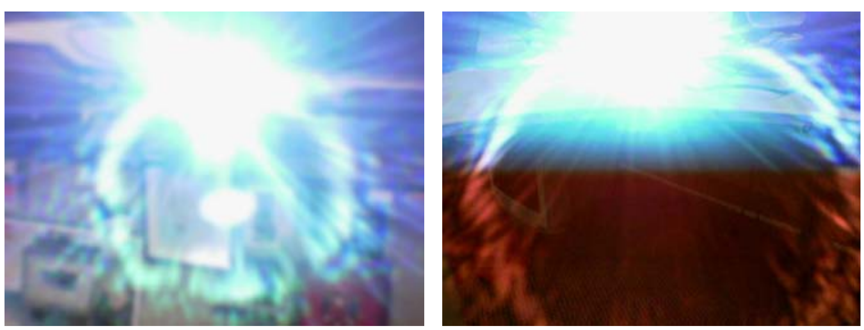


(a) (b)

Figure 3. On the left shows our camera detector unit. We outfitted a Sony HandyCam, placed in *NightShot* mode, with a collection of IR transmitters and covered the lens with a narrow bandpass IR filter. On the right shows our camera detector coupled with a projector to neutralize cameras in the environment.

4.2 Neutralizing Cameras

Once the system detects cameras in the environment, the camera neutralizer component emits localized light beams at each camera lens. This causes a strong reduction in quality of the taken image for several reasons. First, this effect is similar to taking pictures *contre le soleil*, where the concentrated light source overwhelms the picture taken (Figure 4a). Secondly, we emit light beams in a pattern that prevents the CCD cameras from adjusting to the light and prevents the camera from taking a good picture (Figure 4b).



(a) (b)

Figure 4. Images taken from a camera hit by localized light beam emitted by our camera neutralizer. The picture on the left shows a localized light beam generated using a single color. The picture on the right shows a localized light beam generated using color patterns that do not allow the cameras to adjust to the light source (notice the scan line).

4.2.1 Theory of Operation

The camera neutralizer leverages the inherent imperfect sensing capabilities of CCD cameras that result in three specific effects, over-exposure, blooming and lens flare. Over-exposure results in an image which is saturated with light obscuring detail. Blooming occurs when a portion of the camera's sensor is exposed to excessive luminosity, resulting in leakage to neighboring regions. For example, a candle in an otherwise dark setting may cause blobs or comet tails around the flame. Although some cameras are capable of compensating for these effects, they typically only handle moderate amounts of light. Lens flare is caused by unwanted light bouncing around the glass and metal inside the camera. The size of the lens flare depends on the brightness of the entering light. High-end cameras with well-designed and coated optics can minimize, but not completely eliminate, lens flare. By shinning a beam of light at the camera lens, such as that emitted by a projector, blooming and lens flare significantly blocks any CCD camera from capturing the intended image. Digital cameras employ automatic exposure control algorithms, which reduces blooming and flare. However, there is typically a delay before the sensor stabilizes. Thus a flashing light prevents the camera from stabilizing to the light source.

4.2.2 Implementation

To emit a strong localized light beam at cameras, we pair a projector of 1500 lumens with our camera detector. We use the projector to emit localized light beams of an area slightly larger than the size of the reflection. Pixels in the projected image change between white, red, blue, and green. This approach prevents cameras from adjusting to the light source and forces the cameras to take a picture flooded with

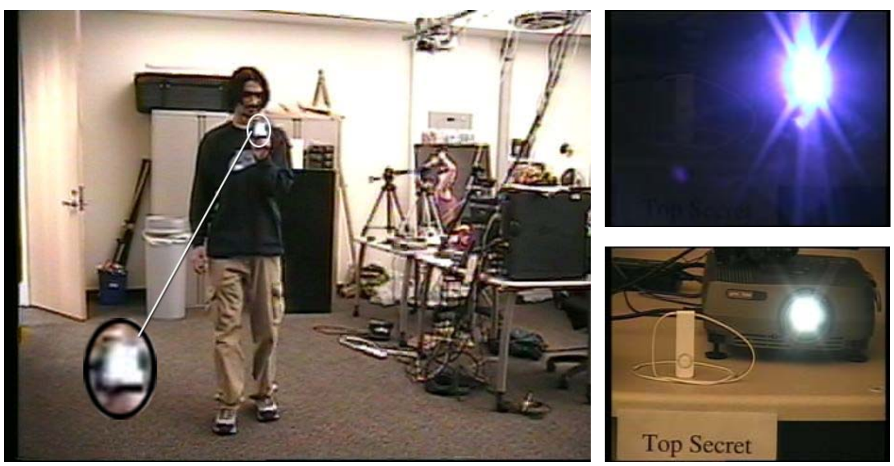


Figure 5. The left shows a camera phone being neutralized by our system (notice the neutralizing light beam over the lens). The top right shows the camera view neutralized by the system, the bottom right shows the camera view when the camera is permitted to capture the view.

light (Figures 4 and 5). In addition, interleaving various projection rates neutralizes a larger variety of cameras. The camera neutralizer continuously emits this light beam until the camera lens is no longer detected. Therefore, this approach works against both still image and video cameras.

We found that the projector can still generate an effective localized light beam when we focus it for up to 5 meters away. Although light from a projector can travel much farther, its luminance decreases with distance. Again, we estimate that 5 meters is roughly the length of a reasonable size for a room. At 5 meters away, we can project localized light beams to cover a pyramidal region with a base of 6 m width x 4.5 m height. To ensure that we can neutralize cameras from all angles, we can measure the angle at which users can approach the surface, and accordingly, we can determine how many projectors we must use to cover that range. We can add additional projectors mounted away from the surface to neutralize cameras from farther away if needed.

5 Assessing the Design Challenges and Limitations

In this section, we present how we addressed our original design goals and the challenges and limitations faced in the design of our system. We also describe how our approach addresses the potential attacks or workarounds people may use to circumvent the capture-resistant environment. Finally, we discuss the known theoretical limitations and the engineering deficiencies in our initial prototype.

5.1 Design Goals

The goals of our capture-resistant environment were:

- to require no need for cooperation or control of the recording devices before, during or after capture;
- to prevent both still images and video; and
- to minimally impact view of the environment by the naked human eye.

Our implementation requires no cooperation or control on the part of the recording cameras. Instead, the environment takes sole responsibility in blocking capture of certain parts of an environment. The capture-resistant environment actively tracks CCD cameras present in the space and blocks them with a localized beam of light directed at the camera's lens. We have designed our system to work with both still and video cameras and have found that our system works on most consumer-level digital camera and all camera phones. Our system has no impact on the human eye other than a slight glow that a person may see coming from part of the environment (caused by the projector). As we will discuss, we can reasonably prevent eyes and eyeglasses from being mistaken for a camera lens. In addition, future implementations of the camera neutralizer will not use projectors and thus would not produce a glow.

In addition, we wanted our solution to allow for two interesting extension:

- allow authorized cameras to record; and
- allow mobile entities, such as a person, to be made similarly capture-resistant.

In our current implementation we can authorize users to take pictures by turning off the system, but this solution does not allow selected camera to take pictures while blocking other cameras.

A simple enhancement to our system would be to use 2D retro-reflective glyphs (Figure 6) to permit certain cameras to capture in the environment. The 2D glyph encodes a unique identifier that allows the system to recognize the camera. The owner of the physical space gives out a tag when she wants to allow a specific camera to capture within that space. The glyph needs to be physically attached near the lens of that camera and would be detected by the camera detector. The system then allows the camera to take pictures in the environment by simply not directing localized light beams at the permitted devices.

Figure 6. A 5 cm x 5 cm retro-reflective glyph pattern is temporarily attached near a camera phone's lens.

Although we do not implement the ability to make moving objects, such as humans similarly resistant, we cam imagine building a wearable version of our camera detector and neutralizer to prevent records on individuals in public spaces. We discuss in the following sections how we can construct a much more lightweight version of the neutralizer component.

5.2 Challenges

There are two types of challenges our system faces. First, we must handle the errors involved in detecting cameras. Second, we must address potential attacks or workarounds people may use to circumvent the capture-resistant environment

5.2.1 Errors in Detecting Cameras

A false positive occurs when the camera detection system mistakenly detects a camera in the environment where one is not actually present. A false negative occurs when the camera detector fails to identify a camera pointing at the capture-resistant space.

Handling false positives

False positives can result from the detection system interpreting reflections from metallic or mirrored surfaces present in the space. Because these surfaces potentially produce the same reflective speckle as a CCD sensor, the system would target a non-existent camera.

False positives are not detrimental to the operation of the system. However, the superfluous projector light produced by the false positive may be distracting or even bothersome for people in the environment. The worst false positive situation occurs when the system incorrectly identifies a region near a person's face as a potential camera, irritating or even harming the person's vision.

We can address these problems by further analyzing the potential camera speckles. For the case of a reflection caused by metallic or other lens-like surfaces we can determine a false positive by inspecting the suspected reflection from multiple vantage points. The reflection caused by the CCD camera is always consistent off its surface, so if the reflection moves in the different vantage point views, then it is not a CCD camera reflection. These other surfaces are imperfect reflectors, which is typically attributed to the surface curvature, such as eyeglasses or imperfect finishes like brushed metal. In our system, can simply use two cameras spaced apart and pointed at the same region to help reduce the number of false positives.

Handling false negatives

Unlike false positives, false negatives are detrimental to the security of the space. One solution is to take a naïve approach and assume that any reflection is a potential camera. This may be appropriate when security is of utmost importance. However, this approach does not work when the CCD camera does not produce a reflection. Occlusion of the CCD from the camera detector is the primary reason for this, but typically an occlusion of the CCD inherently blocks a photograph from being taken in the first place. The camera can be angled sufficiently enough away that the incident light fails to reach the detector camera. In this case, the camera is already turned far enough away such that the capture-resistant space does not appear in its field of view. Thus, if there is no light reflection from the CCD then that CCD camera cannot see the region around the detector.

We can place multiple pairs of camera detector and neutralizer units around a space for added security. From our experience, we have found one pair to be sufficient. A cheaper alternative is to place multiple IR light emitters throughout the space to increase the likelihood for a reflection. This solution may increase the number of false positives; however, its cost effectiveness outweighs those concerns.

5.2.2 Attacks and Workarounds

Aside from physical vandalism to the capture resistant environment, we identify some workarounds users may employ with their CCD camera. We discuss how our system design handles some of these attacks; in many cases, we point out the unobvious ways that our solution inherently addresses the problem. Where appropriate we provide some theoretical justification.

Masks and filters

An attacker may try to mask the camera lens with surfaces like those used in typical sunglasses. These surfaces, however, do not block IR light; thus, our system would still detect the CCD sensors. Mirrored and even polarized sunglasses also fail to prevent the camera detector from finding the CCD. However, sunglasses are effective at mitigating the effects of the neutralizer on the camera. Sunglasses drastically reduce the intensity of the projected light. Despite this reduction, we have found that the light pattern and intensity we used in our system is still effective at neutralizing cameras from capture. A neutralizing beam, such as from a laser, could also solve this problem.

IR filters pose the greatest problems for our particular system. In our current solution, we use pure IR light (880 nm) for CCD sensor detection. An 880 nm notch IR filter could be placed in front of a camera; this prevents IR light from reaching the CCD sensor while still allowing other visible light to pass. We can mitigate this attack with a design that also detects IR filters in the environment and treats them as suspected cameras. An IR filter reflection looks very similar to CCD sensor reflection to our camera detector (the only difference is a larger speckle size), thus making it a straightforward task to detect IR filters and treat them as a camera. However, this solution will result in more false positives. Since IR filters allow visible light to penetrate, the camera neutralizer is not affected by this attack.

Mirrors

A user can avoid pointing a camera at the capture-resistant region by using a mirror and taking a picture of the reflection on the mirror. However, our experience shows that the camera detector can still clearly spot the CCD sensor in the mirror and the camera can be effectively neutralized by aiming back at the mirror.

An attacker could also hide a camera behind a one-way mirror to prevent it from being detected. Similar to the sunglass situation, IR light can still be detected appearing behind a one-way mirror, making it an ineffective attack. In addition, images taken from behind a one-way mirror tend to produce low quality images in the first place.

Modifying Camera Sample Rate

The camera could be pre-programmed to sample at the rate of the neutralizer pattern. This problem can be addressed by interleaving random frequencies for each pixel in the neutralizing projection pattern. In this case, CCD cameras would not be able to synch to the projected pattern and frequency because of its inability to sample each pixel at different rates. This is a fairly straightforward extension to our system, which we have tested independent of our proof of concept implementation.

Another possible workaround is to evade the neutralizing beam by moving the camera faster than our detector tracks. There is a limit to how fast the camera can be moved when taking a picture because of motion blur. The 15 Hz tracking rate of our implementation is sufficient for all camera phones and most digital cameras. High-end cameras with extremely fast shutter speeds require faster tracking. Increasing the area covered by the neutralizing beam would address this problem because of the larger movement needed to move outside the beam of the light.

5.3 Limitations

Our current implementation is limited to indoor environments, although we have found success near widows and areas where there is significant amount of natural light. However, for venues like an outdoor concert, this system would need to be modified extensively to accommodate for such a large setting.

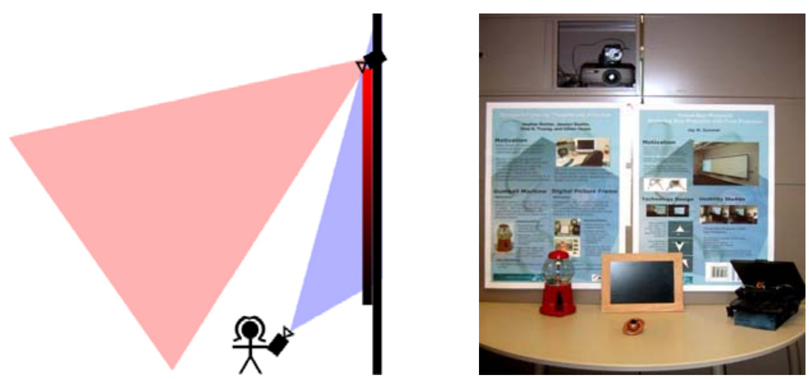
This solution works well with traditional CCD cameras, but may have problems with high-end cameras that have very fast shutter speeds, fast frame rates, and retracting shutter that cover the CCD sensor, such as a SLR. Other capture technologies that do not employ CCD sensors, such as ordinary film cameras, cannot be detected with our system. SLR cameras are still very hard to produce cheaply and we do not expect to see such high-end components integrated into a mobile phone anytime soon. Although the quality and resolutions of camera phones will increase, they do not have a direct impact on the effectiveness of this system (*e.g.,* our system performs just as well on a 4 megapixel CCD digital camera).

Additionally, most camera systems employ some type of optical system; by looking for any reflection from the optical devices, it is possible to detect any camera, including SLRs and ordinary film cameras. However, this approach would increase the false negative rate.

Our current implementation requires manual calibration between the camera dectector and the neutralizer (the projector) to a planar surface. Although we keep the detector camera and projector close to each other, parallax still poses a problem when we move too far in front or behind the calibrated plane. There are two ways to address this problem. The first approach is to use a stereoscopic vision system that tracks in 3D space. The second approach is to make the projector coaxial with the view of the detector camera by using a beam splitter. The first approach provides flexibility in where to place the neutralizer and the camera detectors in the environment, but it requires two cameras. The latter approach requires the neutralizer and camera detector to be collocated, but it only requires one camera.

The conical region of the camera detector poses problem with “dead zones” close to the detector/neutralizer system. A dead zone exists a short distance in front of the protected surface and directly underneath the detector unit (Figure 7a). A person standing in this dead zone will be able to take a picture, although the resulting photo will be very warped. One way to address this issue is to put a physical barrier to effectively limit how close a user can get to the protected region (Figure 7b). The other is to install another neutralizer at a lower level to cover the dead zone. Similar dead zones occur on the azimuth and are handled similar to the elevation solutions.

Our system consists of three significant elements: a camera, a DLP projector, and a PC. This solution costs approximately ~$2500 USD. However, an actual implementation would be significantly cheaper. Video cameras are fairly affordable and will decrease in price with time. The PC is easily replaced with a very inexpensive microcontroller. The projector is the most expensive of the three elements. W used a projector because of the ease in projecting concentrated light at very specific regions. Typical projectors are designed to produce high quality images at high resolutions, have tuner components, and incorporate sophisticated optical components. Our projection region is very small and does not require the level of optical precision and resolution available in typical projectors. We can imagine a projector designed specifically for our application that is significantly cheaper. An even cheaper alternative is to replace the projector with a scanning laser (similar to those found in laser light shows). By spinning a mirror and pulsing different tri-colored lasers, we could produce the same effect as the projector. This is not only a much cheaper solution, but also a more effective solution than a diffuse projector beam. Therefore, it becomes more practical to place many of these systems throughout a space for increased coverage.



(a) (b)

Figure 7. (a) A dead zone exists a short distance in front of the protected surface, directly underneath the detector unit. A user standing in this dead zone will be able to take a picture, although the resulting photo will be very warped. (b) We place a table in front of the surface to obstruct users from entering this dead zone. The right picture shows a sample setup of our system that prevents people from taking pictures of posters in our lab. In this example, the posters and prototypes can be viewed by the human eye, but they can not be captured by cameras within a 45° sweep in the azimuth in front of the table.

6 Conclusions

The increasing ubiquity of cameras, particularly cheap and small CCD cameras raises legitimate concerns about how to make people aware of capture and allow them to prevent unwanted recording. In this paper, we presented a proof of concept implementation of a capture-resistant environment that prevents the recording of still images and movies of regions within that physical space. Our system actively seeks cameras in the environment and emits a strong localized light beam at each device to neutralize it from capturing. Although the directed light interferes with the camera's operation, it minimally impacts a human's view in the environment. Our approach also requires no cooperation on the part of the camera or its owner and it minimally disturbs the natural viewing experience by the human eye. Additionally, we discussed how we can extend the work to permit certain cameras to take pictures in the environment while still preventing others. Although our proof of concept implementation effectively blocks cameras within its 45° field of view for up to 5-10m away, we can easily add additional detector and neutralizer units to prevent a larger sweep from capturing. This implementation allowed us to investigate and address challenges against our approach. We explain how our approach inherently resolves many of the challenges and describe extensions to this work to address others. For example, cost can be significantly driven down by implementing a self-contained unit as we discussed. This work simply presents a proof-of-concept implementation that can be engineered in the future to detect and neutralize camera recording for large environments and even mobile entities, such as a person.

References

1. Brassil, J. Using Mobile Communications to Assert Privacy from Video Surveillance. To appear at *1st International Workshop on Security in Systems and Networks 2005*. April 2005.
2. Art. 29 Data Protection Working Party. Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance. Document 11750/02/EN WP89, European Commission (2004). http://europa.eu.int/comm.
3. Chung, J. Threat Of Subway Photo Ban Riseth Again," Gothamist, 2004 November 30.
4. Eagle Eye. Bulletin of the Connecticut Academy of Science and Engineering. Vol. 12, No. 2, 1997.
5. Halderman, J.A, Waters, B., and Felten E.W. Privacy Management for Portable Recording Devices. *In The 3rd Workshop on Privacy in Electronic Society (WPES 2004).* Washington, DC. October 2004.
6. Iceberg's Safe Haven. http://www.iceberg-ip.com/index.htm.
7. Perry, S. HP Blur Photos with Camera Privacy Patent. http://www.digital-lifestyles.info/display_page.asp?section=business&id=1888. January 2005.
8. Video Voyeurism Prevention Act of 2004. 18 USC 1801. December 2004.
9. Wagstaff, J. Using Bluetooth To Disable Camera Phones. http://loosewire.typepad.com/blog/2004/09/using_bluetooth.html. September 2004.

Video Figure

A video figure supplementing this document, showing our proof of concept implementation can found at:

http://www.zolan.org/cre/

These videos are DIVX encoded. (The necessary codec and player can be found at http://www.divx.com)