SAND2014-18064C

Authentication Approaches for Standoff Video Surveillance

George Baldwin, Shane Sickafoose, William Sweatt, and Maikael Thomas

Sandia National Laboratories
Albuquerque, NM 87185-1373 USA

Abstract. Video surveillance for international nuclear safeguards applications requires authentication, which confirms to an inspector reviewing the surveillance images that both the source and the integrity of those images can be trusted. To date, all such authentication approaches originate at the camera. Camera authentication would not suffice for a "standoff video" application, where the surveillance camera views an image piped to it from a distant objective lens. Standoff video might be desired in situations where it does not make sense to expose sensitive and costly camera electronics to contamination, radiation, water immersion, or other adverse environments typical of hot cells, reprocessing facilities, and within spent fuel pools, for example. In this paper, we offer optical architectures that introduce a standoff distance of several meters between the scene and camera. Several schemes enable one to authenticate not only that the extended optical path is secure, but also that the scene is being viewed live. They employ optical components with remotely-operated spectral, temporal, directional, and intensity properties that are under the control of the inspector. If permitted by the facility operator, illuminators, reflectors and polarizers placed in the scene offer further possibilities. Any tampering that would insert an alternative image source for the camera, although undetectable with conventional cryptographic authentication of digital camera data, is easily exposed using the approaches we describe.

1. Introduction

There are situations in international nuclear safeguards applications where video surveillance monitoring may be of interest, yet the environment is not advisable for sophisticated camera electronics. Hot cells are an example, because of potentially high radiation levels. However, radiation is not the only concern; radioactive contamination, toxic atmospheres, high temperatures and similar conditions exist in various nuclear fuel cycle facilities.

Even if the conditions are not normally a problem for the camera itself, they may complicate matters for the installation and servicing of the camera by human inspectors. Periodic physical access to the camera is also important where cameras are enclosed in tamper indicating enclosures that must be checked visually by safeguards inspectors. Video surveillance cameras that meet safeguards requirements are typically expensive; they cannot easily be treated as disposable hardware.

Standoff Video

We therefore developed the concept of "standoff" video surveillance [1] with the idea to separate the surveillance camera into an extended instrument with three distinct pieces: 1) the front end, consisting of the minimal optical components necessary to produce an image of the scene under surveillance, 2) the back end, consisting of everything else, especially the sensitive image sensor and associated electronics, and 3) the standoff,[1] which conveys the acquired image of the scene between the front and back end of the instrument. Figure 1 illustrates the concept.

Note that the standard (or fisheye) camera lens no longer works. Instead, we replace it with a *relay* lens, which serves only to couple the remotely-acquired image to the camera's CMOS image sensor. Compared to the standard camera lens, the relay lens has a longer focal length and a greater separation from the image plane.

[1] *Note that here we use the term "standoff" to refer to the distance behind the objective lens, not in front of it. It has nothing to do with how far away the surveillance system is from objects in the surveillance scene.*

Although not shown in Figure 1, the standoff section between the objective optics and the camera should be enclosed in a non-reflective, opaque-walled pipe to exclude ambient light from the camera.

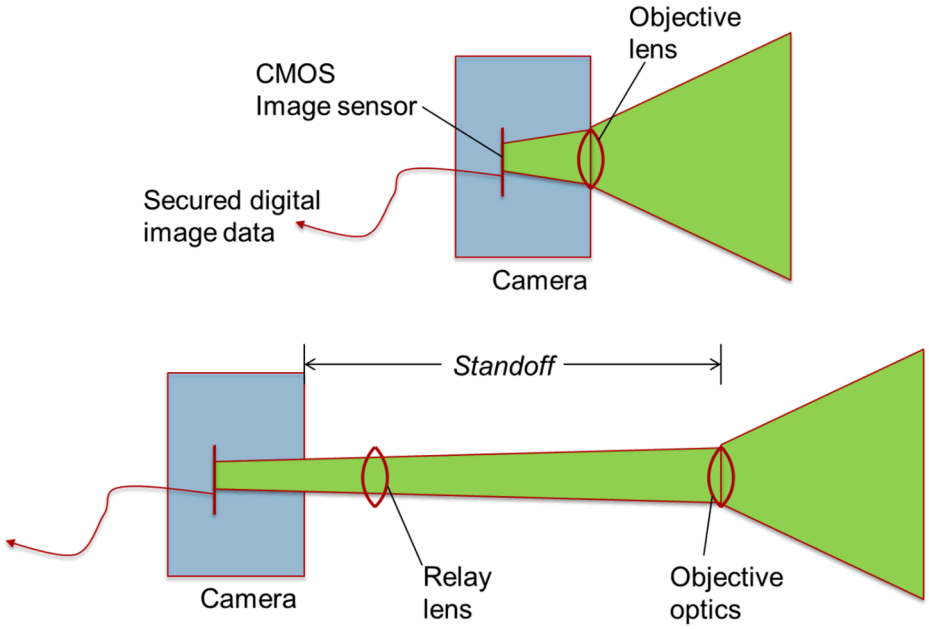

Figure 1. Standoff video surveillance (lower picture) separates the objective optics and image plane of a standard video surveillance camera (upper picture)

Another adaptation for standoff video, important for high radiation applications, is to use reflective optics (mirrors) rather than refractive optics (lenses) for the objective. Figure 2 illustrates the concept. Three mirrors enclosed in a box at the end of the standoff comprise the objective optics. The mirrors are much more radiation hard than any glass or plastic lens. The mirrors are the only part of the surveillance system inside the radiation area; the rest of the surveillance system is outside of the radiation area, protected behind a shield wall. In principle a pass-through would include path offsets to prevent radiation streaming; in that case images can still be relayed through the standoff using mirrors, as appropriate.

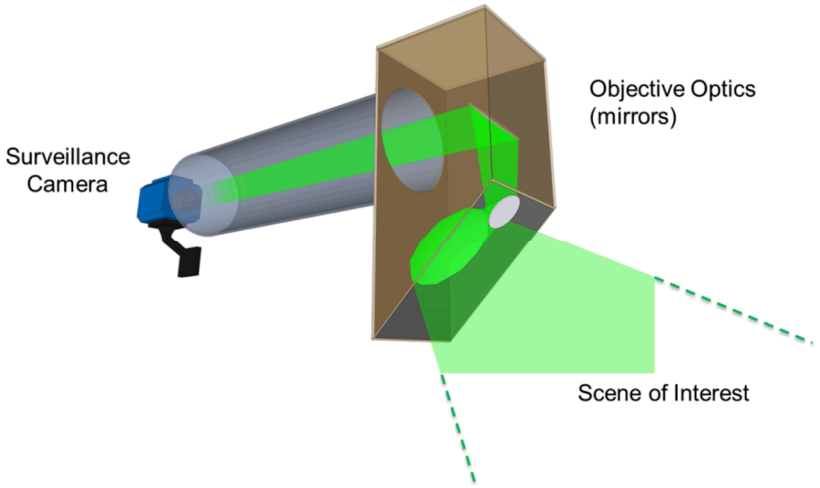

Figure 2. Standoff video with reflective optics, using two flat mirrors and a concave mirror for the objective

2. Authentication of video surveillance images

Particularly for international nuclear safeguards, a fundamental problem for video surveillance is being able confidently to answer the question, "How can we be sure we're looking at what we think we are?" In the popular fictional movie *Ocean's Eleven*, [2] thieves are able to enter a casino vault despite being under the watchful eyes of surveillance cameras. They succeed because the security personnel are instead watching pre-recorded data, rather than live video. Such a "replay" attack is one example of the kind of threat that authentication is intended to prevent.

By *authentication* we mean any methods employed to ensure that (1) a video feed is indeed coming from the expected source, (2) at the expected time, and (3) that the images have not been modified in any way.

For safeguards applications of video surveillance, the camera protects its security-critical component(s) within a tamper-indicating enclosure (TIE). Within the TIE, close to the CMOS sensor, cryptographic means "sign" the video image data, before the data are communicated to the inspectorate for review. An inspector is later able to validate the signature, which confirms both the source and the integrity of the image data. For other applications requiring image authentication, various proprietary methods or embedded "digital watermarks" have been used. [3][4]

Note that normal cryptographic signing of video data begins at the camera; it does not address "before the lens" tampering. If someone is able to alter what the camera is able to see, such as by inserting a static photograph of the scene, the cryptographic authentication method will not detect it. To some extent, that risk can be mitigated with system approaches. For example, one might deploy multiple cameras, where each camera can also include another within its field of view.

3. Authentication of standoff video images

Standoff video exposes even more of the surveillance system to the risk of tamper, because of the extended optical path, as suggested in Figure 3.

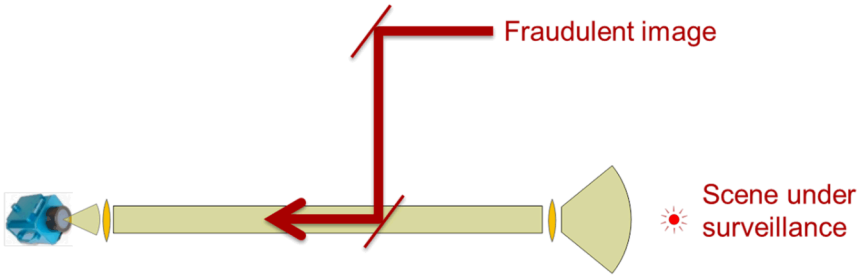

Figure 3. Risk of tamper with standoff video surveillance

As already mentioned, no authentication method applied to digital image data would be able to detect such tampering. Our only recourse is to devise a means to authenticate the part of the surveillance system in front of the CMOS image sensor, before the optical image has been converted to a digital data stream. Fundamentally, the problem calls for an optical approach to self-interrogate the optical path: in some way, illuminate the scene in a deliberate, unpredictable way and confirm that the imposed signal indeed appears in the acquired image.

4. In-scene image authentication

There may be information already within a viewed image scene that already may be relevant to authentication. A clock is an obvious example of something that provides time varying information. It is of limited value, however, since its owner can set it to report any time. In most cases, it will be necessary for the user of the surveillance system to insert something remotely-controllable in the scene, which lights up, moves, or otherwise reacts in a way that can be detected in the surveillance image. Such an approach would require additional access beyond just that required for the surveillance camera. For standoff video applications, the scene under surveillance may be hazardous, so it would be best not to depend on placing additional hardware within the surveillance scene just to support authentication.

However, there is one thing that we can easily place in the scene: light. We can shine light through much the same path as the image follows, but in the opposite direction. Our approach involves illuminating particular spots within the surveillance field of view, in various unpredictable ways. As desired, we could vary the color, turn the light on and off, vary the brightness, or change the number, location and size of illuminating spots. In any case, we can effect a change in the visual appearance of the scene in a known fashion, and then validate the scene by looking for an expected response in the image. We refer to this approach as *dynamic optical watermarking*. The possible use of shadows, reflective surfaces, and other scene features may add to the complexity of the authentication.

The authentication light sources could in principle be either diode lasers or light emitting diodes (LEDs). Lasers would have ample brightness for deep scenes with relatively distant objects, but have practical issues involving eye hazards. For that reason, they might not be acceptable to facility operators. We therefore choose to work instead with LED light sources, although the system implementation will need to contend with beam divergence and brightness.

Note that the resulting watermark in the image does not need to be obviously bright to the human eye; it merely needs to be detectable by automated software using a change-detection algorithm to compare images on pixel-by-pixel basis.

In practice, we envision that video surveillance image acquisition would consist of at least several frames, where each frame differed from another by the particular watermark that had been imposed by the authenticating light source. Thus the light source(s) would need to be synchronized with the camera frame acquisition, and the various parameters used to control them included with the metadata for the acquired frame. Implementation would include a trusted means to randomize the authentication light parameters.

5. Experimental tests

We have assembled an experimental mockup of a simplified “baseline” scenario for standoff video surveillance, which is pictured in Figure 4. We adapted a safeguards video surveillance camera, the DCM-C5, and replaced the camera objective lens with a 225 mm focal length relay lens approximately 29 cm from the camera’s image plane. The standoff distance is approximately 2 m. All of the optical components for the standoff system are 50 mm diameter, which should provide adequate light collection for anticipated applications.

Although we would normally enclose the entire standoff in an opaque-walled pipe to exclude ambient light, the figure shows that we have only blocked the section between the camera image plane and the relay lens. (Note that the narrow-diameter tube behind and parallel to the standoff image path encloses only the authentication light.) Even so, it is clear from the

DCM-C5 built-in display that the scene being viewed (the objective optics of the system point at the tool box in the background) is clearly visible above any background light.

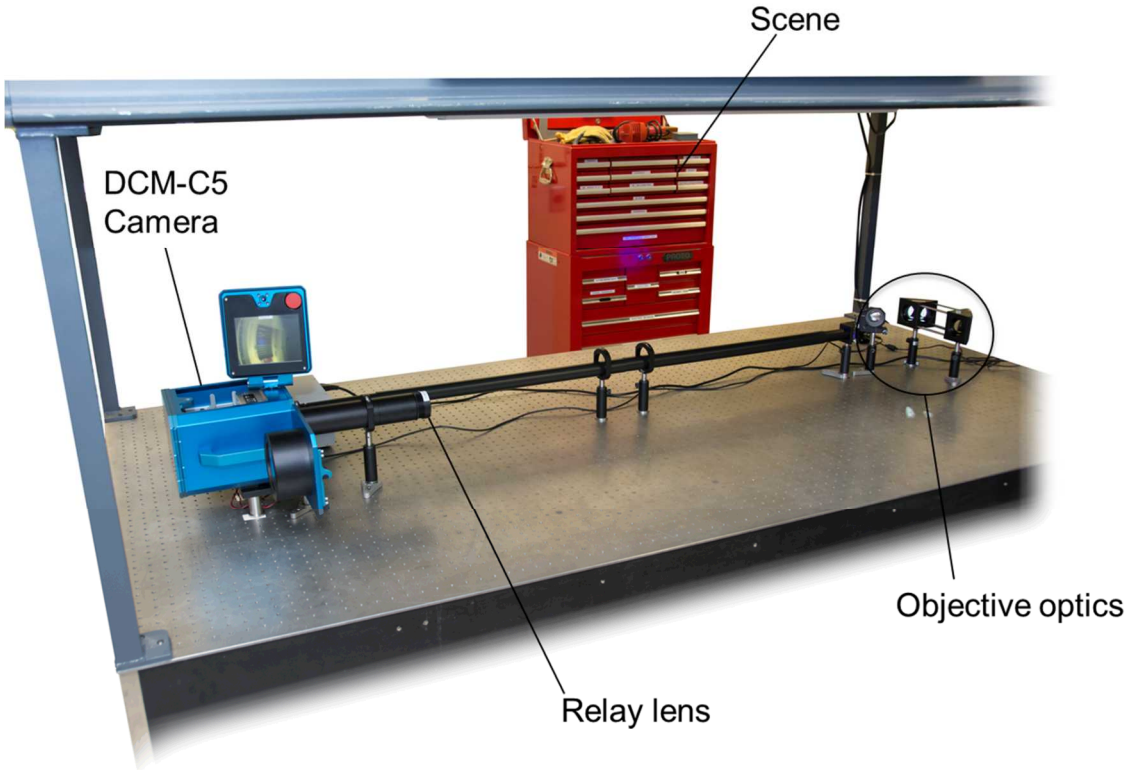

Figure 4. Experimental baseline scenario to demonstrate standoff video with optical authentication

Figure 5 shows a closer view of the front end of the experimental setup from another angle. (In this picture, we are now standing between the tool box and the optical bench.) The rightmost of the three mirrors that comprise the objective optics is concave, with a 100 mm focal length. The curvature enables the system to subtend about a 45° view of the scene.

On the right, at the end of an enclosed tube, is a flat mirror that reflects the LED light onto the scene. The LEDs themselves are not visible here, but are located near the DCM-C5 camera. We are working with four different wavelengths:

455 nm	1 W
625 nm	700 mW
735 nm	300 mW
850 nm	1 W

It may not be possible to discern from the figure, but a single blue spot roughly in the center of the toolbox was clearly visible to the naked eye even in the brightly lit room. As noted previously, such an authentication spot does not need to be so bright to be detectable with change detection software. It should be clear that changing the color, by powering a different LED, turning the authentication light on or off, are all easy to accomplish. We are currently working on ways to change the number, location and size of authentication watermark spots using various additional optical components, but that is beyond the scope of this paper.

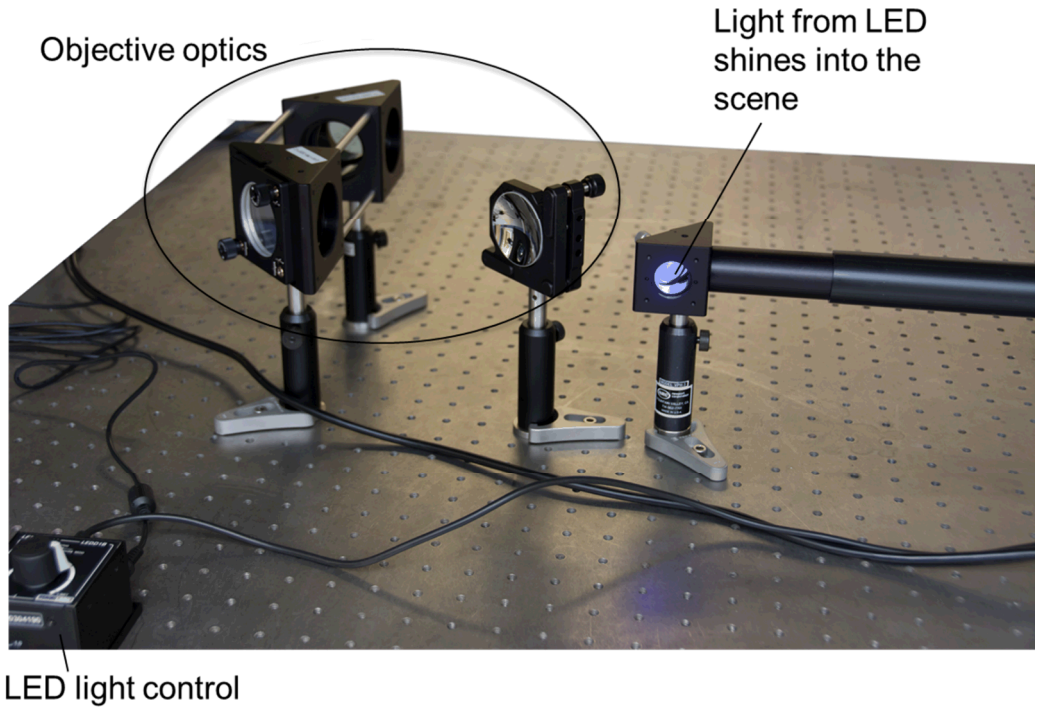

Figure 5. Front end detail of the experimental standoff video system

6. Discussion

The dynamic optical watermarking approach to authenticating standoff video surveillance images is especially attractive, because the authenticating hardware can be packaged together with the surveillance camera; no separate hardware must be placed in the scene.

We envision two separate development paths for future work.

One would be to develop standoff video surveillance. Additional engineering is needed to enclose the objective optical components in a unified housing, able to be coupled to the end of the standoff pipe and having a window to the surveillance scene. It would further incorporate the optics for reflecting the authentication light into the scene. We envision either the separate parallel pipe for the authentication light, or instead sharing the image standoff pipe in a "crossed beam" arrangement.

Various deployment scenarios can be imagined for standoff video. Surveillance of a hot cell might consider passing the standoff path through an existing leaded glass, oil-filled windows. Standoff pipes could be used underwater in spent fuel pools to bring the objective optics closer to items under surveillance. It may be possible to design an articulating front end with pan/tilt capability, or even a movable boom with a jointed arm.

Standoff video surveillance might further be considered as a way to multiplex image feeds from separate objective optics to a single shared camera. A switching element is all that would need to be added.

A second development path would be for the authentication approaches based on dynamic optical watermarking. This can be pursued for any video surveillance, not only standoff video. We still need to automate image processing to extract the watermark from frame differences

in the image, but this should be rather straightforward. We need to synchronize the authentication source with the camera image acquisition, and incorporate the authentication parameters in surveillance image metadata. Various means would increase the sophistication of the projected watermark spots in the scene, especially their temporal and spatial variation.

7. Conclusion

Through this work we have explored new concepts for video surveillance in hostile environments, using standoff. Standoff video surveillance is a viable means to acquire images to protect sensitive camera electronics by minimizing the part of the system that is exposed to hazards such as high radiation. Standoff video surveillance even enables the multiplexing of separate surveillance scenes to a single camera.

We have further investigated the additional steps needed to authenticate standoff video images, since conventional digital cryptographic approaches for signing data may be insufficient. Dynamically illuminating a scene with a watermark is a promising approach for optical authentication of video surveillance images, and could just as easily be applied to conventional (non-standoff) video surveillance.

8. Acknowledgment

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. Support to Sandia National Laboratories provided by the NNSA Next Generation Safeguards Initiative is gratefully acknowledged. We greatly appreciate contributions to this work from Jason Bolles, Ron Goeke, Mark Johnson, and Ron Mori.

SAND2014-XXXX

REFERENCES

[1] George Baldwin, William Sweatt, and Maikael Thomas, Standoff Video Surveillance for High Radiation Applications, proceedings of the 55th Annual Meeting of the Institute of Nuclear Materials Management, Atlanta GA, USA, July 21, 2014, SAND2014-15052C, http://www.inmm.org/source/proceedings/files/2014/a452_1.pdf

[2] *Ocean's Eleven*, http://www.imdb.com/title/tt0240772/

[3] *Hackers crack Nikon's image verification system*, Homeland Security News Wire, 4 May 2011, http://www.homelandsecuritynewswire.com/hackers-crack-nikons-image-verification-system

[4] Gwo-Jong Yu, Chun-Shien Lu, and Hong-Yuan Mark Liao, *Mean-quantization-based fragile watermarking for image authentication,* Opt. Eng. 40(7), 1396-1408 (Jul 01, 2001), http://opticalengineering.spiedigitallibrary.org/article.aspx?articleid=1098272#