Analog Video Authentication and Seal Verification Equipment Development

Savannah River National Laboratory

G.E. Weeks

M.H. Phillips

Pacific Northwest National Laboratory

J.E. Tanner

J.M. Benz

Idaho National Laboratory

G.D. Lancaster

Milagro Consulting, LLC

K.M. Tolk

Under contract to the US Department of Energy in support of arms control treaty verification activities, the Savannah River National Laboratory in conjunction with the Pacific Northwest National Laboratory, the Idaho National Laboratory and Milagro Consulting, LLC developed equipment for use within a chain of custody regime. This paper discussed two specific devices, the Authentication Through the Lens (ATL) analog video authentication system and a photographic multi-seal reader. Both of these devices have been demonstrated in a field trial, and the experience gained throughout will also be discussed.

Typically, cryptographic methods are used to prove the authenticity of digital images and video used in arms control chain of custody applications. However, in some applications analog cameras are used. Since cryptographic authentication methods will not work on analog video streams, a simple method of authenticating analog video was developed and tested.

A photographic multi-seal reader was developed to image different types of visual unique identifiers for use in chain of custody and authentication activities. This seal reader is unique in its ability to image various types of seals including the Cobra Seal, Reflective Particle Tags, and adhesive seals. Flicker comparison is used to compare before and after images collected with the seal reader in order to detect tampering and verify the integrity of the seal.

1. Background

Verification of compliance with nuclear dismantlement treaties has always been a difficult problem. Neither side is willing to disclose weapons design details. As such, the monitoring party is not allowed to view the device that is being dismantled or any of its components. Further any measurements that would reveal classified information such as size, geometry or isotopic composition of the physics package are also not allowed. Without being able to physically see the weapon and measure the specific characteristics of the physics package, it is nearly impossible to ascertain with certainty that it actually is a nuclear weapon. As should be obvious to the most casual observer, this presents a significant challenge for the monitoring party. In response to this problem, confidence building methods have been developed to provide reasonable assurance that weapons are actually being dismantled and removed from service. These confidence building methods are based on radiological attribute measurements utilizing information barriers that protect against disclosure of classified information and a strong Chain of Custody (CoC) regime.

Non Destructive Assay (NDA) methods are typically used to determine whether the physics package has a pre-negotiated set of attributes that would give the monitoring party high confidence that the device is actually a nuclear weapon. However, unprotected NDA measurements would also reveal classified information that the monitoring party is not allowed to have. Information barriers are used to allow the required information to be collected and automatically analyzed, but only give the monitoring party a “Yes” or “No” answer as to whether the device in question has this pre-negotiated set of attributes.

Once the monitoring party is confident that the device in question is in fact a treaty controlled item, CoC methods are used to control access to the device to ensure that this specific device moves through the dismantlement process and all of its constituent parts are properly stored or destroyed in accordance with treaty requirements. The CoC regime is comprised of the equipment, methods and procedures that are used to control access not only to the treaty controlled items and their constituent parts, but also the facilities and equipment used during the dismantlement process. Of necessity the CoC regime is very complex and uses every available means to detect non-compliance with negotiated treaty requirements.

The specific NDA and CoC methods used vary from treaty to treaty and are beyond the scope of this paper. This paper will focus on equipment designed to solve two specific CoC problems: authentication of analog video streams and a reflective particle tag reader that will service multiple seal types.

2. Summary

Containment and Surveillance are two important aspects of any CoC regime. This paper discusses two devices designed to improve the security of classical containment and surveillance methods. The first of these devices is Authentication Through the Lens (ATL). With available photo editing software, unprotected analog video streams cannot be trusted. It is too easy to intercept the video signal and modify it to conceal nefarious activities. This problem can usually be resolved by using digital cameras and cryptographic authentication methods to verify that the video stream has not been altered. However, it is not always possible to use digital video cameras. Therefore a means to authenticate an analog video stream was needed. The ATL device impresses an authenticated digital message in the analog video stream. While this does not preclude tampering with the video, it does make tampering much more difficult and ensures that evidence of the tampering remains in the video stream after the fact.

The second device is a photographic seal reader that was fitted with a number of adaptors to enable the verification of multiple seal types. Adaptors were developed for the QuickSeal, Cobra, and adhesive seal. The adhesive seal and the QuickSeal were modified by adding a variant of the Reflective Particle Tag[1,2] (RPT) as a unique identifier. The RPT, originally developed by Sandia National Laboratories, and its variants remains one of the strongest optical unique identifiers available. The RPT uses small reflective particles embedded in an epoxy binder to generate a strong unique identifier. The light reflecting off of the randomly distributed particles generates a reflective pattern that is not only unique for each application, but is also unique for each illumination angle and virtually impossible to counterfeit. The Change Detection System (CDS), developed by Idaho National Laboratory was used to compare reference and verification images for each seal. CDS compares two pictures that were taken from similar angles with similar magnification and lighting. CDS automatically corrects small differences in angle and magnification and then does a flicker comparison (flashes back and forth between the two images). This method is very useful in identifying very subtle differences between images. These differences seem to flash on and off during the comparison. To make the RPT signature more secure, reference and verification images are taken at multiple illumination angles.

[1] *International Security News*, Volume 7, Number 1, pg 11, June 2007, Sandia National Laboratories.

[2] Keith M. Tolk, “Reflective Particle Technology for Identification of Critical Items,” Proceedings of the 33rd INMM Annual Meeting, Orlando, Florida, 1992, pp 648-652

These two devices were developed for use in an international monitored weapons dismantlement exercise. Experience using each of these two devices in a realistic dismantlement scenario will be discussed. However, no specifics about the location, scenario or exercise results will be discussed.

3. Authentication Through the Lens (ATL) Device

3.1. Purpose

In arms control applications, both sides need to have the utmost confidence in the security and accuracy of any video surveillance information used for treaty verification. Normally, digital video cameras are used and each video frame would be authenticated by appending a Message Authentication Code, commonly referred to as a CMAC[3]. However, some applications require the use of analog video cameras.

Analog video streams cannot be authenticated using normal cryptographic methods. The ATL is a proof-of-concept prototype developed to provide reasonable assurance that an analog video stream could not be altered without leaving tamper indications that could be identified using standard photograph examination tools. The ATL is a specially designed digital clock that is physically placed in the surveillance scene. See Figure 1 below. The clock displays the time in a binary format along with a CMAC generated from the time and date. Each frame then has an authenticated time stamp embedded in the image that serves as a unique signature. Since each frame has a unique signature embedded in the scene, many classic video attacks such as replaying a video loop are no longer credible threats.

[3] NIST Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication,* Morris Dworkin, May 2005, National Institute of Standards and Technology.

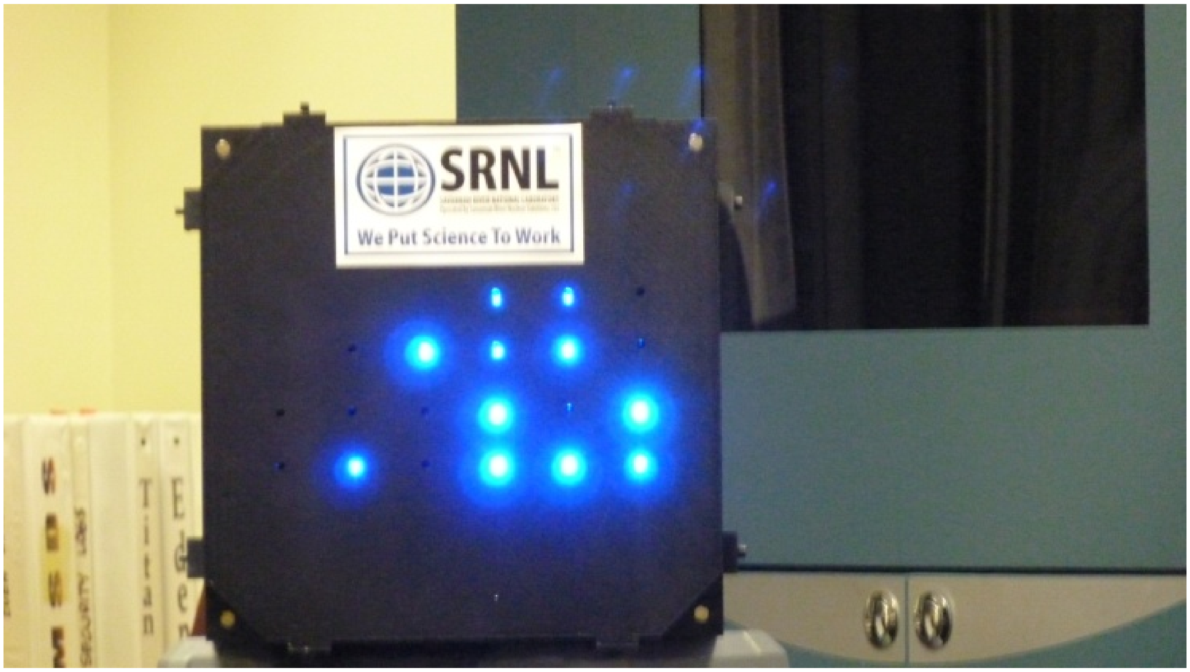

Figure 1 - ATL Device

3.2. Equipment Selection

For simplicity, the ATL prototype was based on a commercially available microcontroller board and a separate Real Time Clock (RTC) module. The microcontroller was selected because it was inexpensive and had enough storage and processing capability to implement the cryptography required to generate the CMAC. The board also had adequate I/O to drive the display LEDs and a 32 character LCD display. The RTC provides accurate date and time information, relieving the microcontroller from the time keeping task.

3.3. Design and Fabrication

The ATL system is comprised of the authenticated clock in the field of view of one and only one surveillance camera. An early analysis of the system identified the need to obscure the ATL information from view by any surveillance cameras other than the one camera it is paired with. This prevents the adversary from capturing the authenticated time information from the ATL and replicating that information in a false scene. Further, the video cables from all of the ATL cameras also need to be under surveillance or maintained in tamper indicating conduit to ensure that they cannot be diverted to cameras looking at false scenes.

A collimator was used on the display LEDs to limit the field of view where all of the LEDs could be seen simultaneously. The collimator was designed to limit the view 15 feet from the ATL to an 18 inch circle.   An 18 inch opaque disk was also installed behind the camera lens to ensure the ATL information could not be viewed from behind the ATL camera.

3.3.1. Enclosure

The ATL prototype was housed in a simple metal enclosure that was modified to allow application of a tamper indicating device to detect opening. This metal enclosure was placed in a plastic collimator discussed in section 3.3 above. The collimator was constructed using plastic tubes to channel the light from each display LED to the ATL face plate. An adjustable frame was used to adjust the alignment between the ATL and the surveillance camera.

3.4. Operation

When powered, the ATL goes through a power-on self-test checking the operation of each of the display LEDs and allowing the operator to set the RTC, see Figure 2 below. Once the clock is set, the time and date are maintained by a small on-board battery. This battery will maintain clock operation for 10 years. After the clock has been set, the operator is prompted to randomly push the "KEY" button a number of times to generate a truly random 128 bit key. This key is generated by the ATL and must be recorded and maintained to be able to validate the authentication code for each time sequence. Please refer to reference 3 for the CMAC authentication method. Once the key is generated and recorded, the ATL is closed and sealed to prevent further tampering. The ATL is then installed in the surveillance field and aligned with its surveillance camera.

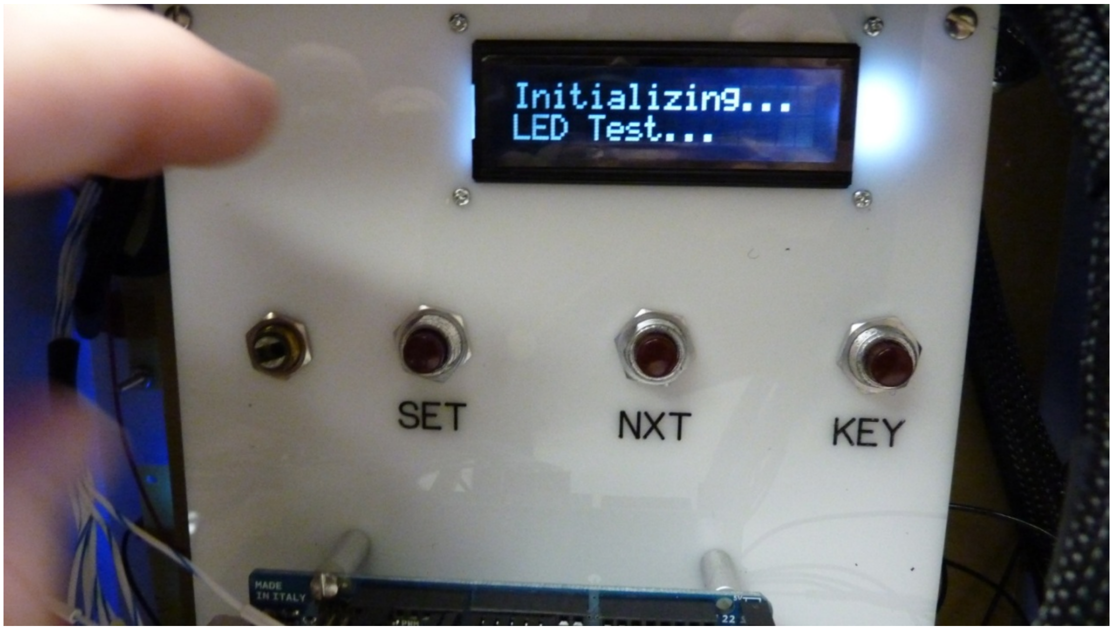

Figure 2 - Power On Self Test

In normal operation each surveillance video frame includes the authenticated time stamp displayed on the ATL. Software was developed to extract this authenticated time and check the CMAC in the video frame with a CMAC calculated using the visible time information from the video frame and the key recorded from the previous initialization of the device. If the two CMAC codes match, the frame has not been replaced. Using the known frame rate of the video camera and the time stamp in each frame, it can be easily seen if frames have been removed. Further, using common video inspection software, it can be seen if each frame has been edited or modified.

3.5. Testing

Initial testing showed that the concept worked, but was difficult to align. As can be seen in Figure 1 above, the collimator causes “blooming” of some of the display LEDs while suppressing others. This is largely an alignment issue. The system is too dependent on positioning of the camera with respect to the ATL device. As it turns out, the distance from the camera is nearly as critical as the alignment between the camera and the ATL. That being said, the reader software was able to accurately interpret the light display, even with the “blooming” effect.

Operational issues related to the Certification/Authentication of the device were also identified. Once the device was certified by the host facility, no computers could be attached to the device without voiding the Host’s certification. As a result, it was not possible to download the key after the ATL was initialized. This required the key to be manually typed into the key database, which presents the possibility for typographical errors as well as key security issues. For additional information see section 6.1 below.

4. Seal Reader

4.1. Purpose

Because a number of different types of seals needed to be imaged, a single Seal Reader device was designed. This device used interchangeable adapters to accommodate different seals such as the Cobra Seal, Reflective Particle Tags, and adhesive seals. This single device is intended to greatly simplify the job of the inspector. No specific camera knowledge is needed in order to obtain consistent high quality photographs. A photograph is taken when the seal is first installed, at designated inspection intervals, and just before the seal is removed. These images are compared using Change Detection Software (CDS) developed by the Idaho National Laboratory (INL). Any change between the initial photo and subsequent photos may be an indication of tampering. Consistency is extremely important when imaging the various seals so that subsequent images can be compared back to the reference image.

4.2. Equipment Selection

One of the problems with building camera-based seal and tag readers is that the commercially available cameras change rapidly. If a reader is designed around a specific camera, it may require extensive redesign when that particular camera is no longer available. A digital single lens reflex (DSLR) camera was selected because it is the most stable camera design available. Even if a specific camera goes out of production, its replacement will have a similar design layout and comparable dimension. Changing from one model to the next should only require changing a spacer to accommodate different lens to base dimensions and adjustment to for differences in the location of the tripod mounting screw. The camera used was a Sony Alpha 500, mainly because it could be easily controlled by a wired connection to the microcontroller. It also had good resolution, a good assortment of available lenses, and the cost was reasonable. This camera was discontinued during the design process, and initial testing was performed using its replacement, the Alpha 33. The next replacement, the Alpha 35 was used for the field exercise.

The camera was used with a standard 50 mm lens with 48 mm of extension tubes added to give the necessary field of view. The lens was always left manually focused at infinity because the camera automatically returns the lens to that position when turned on.

Focusing was accomplished by adjusting the spacing between the camera and the seal surface. The camera was mounted in the reader with a quick release mount so that the camera could be used for other purposes.

4.3. Design and Fabrication

The Seal Reader was designed in Pro-Engineer CAD software. The design consists of a main body, electrical compartment cover, LED light box attachment, and an assortment of adapters for the various seals.

The main body supports the camera and houses the electrical components. The camera is attached to the seal reader body via a tripod quick release plate that attaches to the bottom of the camera via the standard ¼-20 tripod screw thread. This allows the operator to easily remove the camera from the seal reader in order to access the battery and memory card compartments. The quick release plate also ensures that the camera’s position is consistent when it is reattached to the seal reader body. The bottom of the seal reader body is hollow and houses the electrical circuitry of the reader. A plastic cover is screwed into place over the compartment. A button and knob are installed on the main body to allow the operator to control the LED light level and start the image capture process. A photo of the Seal Reader is shown in Figure 3.

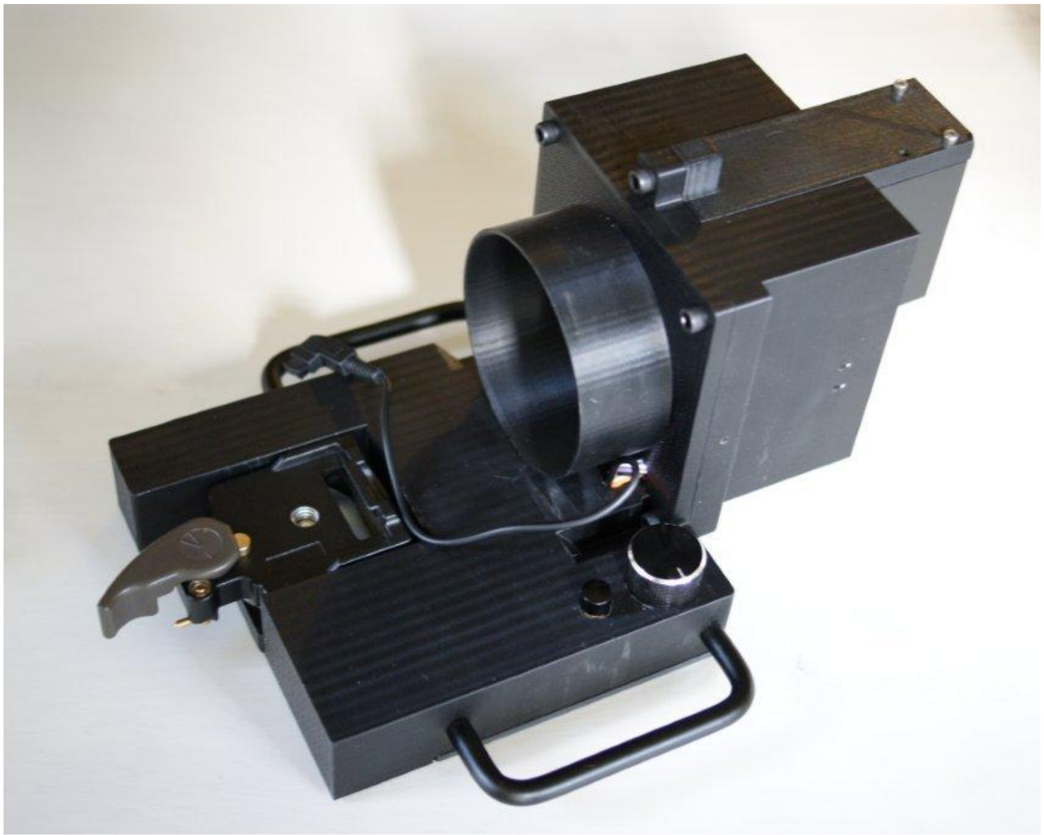

Figure 3 - Seal Reader (No Camera)

The LED light box attaches to the front of the main seal reader body. It houses four LEDs, in opposite corners of the box, which illuminate the subject and can each be controlled independently by the reader’s circuitry. The advantage to four LEDs is that it allows the subject to be lit from four different directions. This is essential when imaging random patterns of reflective particles. The flat face of the LED box can be placed directly onto a surface for imaging. There is a microswitch on the front of the box that is depressed when placed flat against a surface. When the microswitch is activated, the seal reader’s circuitry powers on the camera and readies the device for imaging.

Several adapter attachments were also designed and fabricated to allow for the imaging of various seals. These attachments connect to the face of the LED box via a thumb screw. The thumb screw allows the user to easily change adapters in the field without any special tools. These adapters are described in more detail in the following section.

The components of the Seal Reader were fabricated in the SRNL Rapid Additive Manufacturing (RAM) Lab with a fused deposition modeling (FDM) rapid prototype machine. The plastic prototype parts were used in the field exercise. An advantage to using plastic rapid prototyped parts is that they are lightweight yet durable, and replacement parts can be fabricated very quickly as needed. The rapid prototype parts are also very inexpensive in comparison to the traditional machining of parts.

4.4. Adapters

Three custom adapters were designed for this field exercise. One adapter was designed for the Cobra Seal and two for the Quick Seal. Because the Quick Seal is very small, two different adapter designs were made to test during the field exercise. These adapters allowed the seal to be photographed consistently each time. When the seal was fully placed into the adapter, a microswitch was activated to power on the system. The design of the Seal Reader also allows the user to place the front of the light box directly onto a flat surface for imaging as well. This was the method used for the Adhesive Seals. Unique identifiers such as reflective particles and signatures were applied to adhesive seals and were then imaged using the Seal Reader.

4.5. Operation

The Seal Reader was designed to have a relatively simple operating procedure so that it would be easy enough to use for someone in the field while wearing gloves. It also needs to be easy to use for multiple operators with varying levels of photography knowledge. Each of the adapters has a microswitch on it so that when a seal is inserted, the switch is depressed and automatically powers on the system. If no adapter is attached, a microswitch on the front of the light box will engage when the flat surface of the box is pressed against another flat object. If the flat surface is used to image an object, the operator must use reference marks or features for alignment.

If needed, the focus of the camera can be adjusted using the focal ring on the lens. Next, the knob on the base of the main housing is used to adjust the lighting intensity of the LEDs. Imaging begins when the user presses the red button on the right side of the seal reader. Images are automatically taken with different lighting schemes and saved to the camera’s secure digital (SD) card.

4.6. Testing

The Seal Reader was tested by Milagro Consulting before it was shipped out for the field exercise. This testing consisted primarily of verifying that suitable adjustments could be performed and that the alignment of the camera was correct. Minor issues were corrected, satisfactory images were obtained, and the quick release hardware was mounted. The dimensions of the Alpha 33 and the Alpha 35 cameras were nearly identical, so only minor adjustments were required before the field exercise.

4.7. Flicker Comparison using Change Detection Software (CDS)

The INL Change Detection System (CDS) was used to align images of seals acquired with the Seal Reader camera. There were 4 Cobra Seals and 45 Quick Seals measured during the field exercise. The Seal Reader assembly worked very well as a system to acquire images suitable for alignment with CDS.

There are several issues related to the optimal alignment with the CDS software. The software has two alignment modes, automatic and manual. The software will align the images without any user input in the automatic mode if the images occupy a similar field-of –view (magnification, spatial and rotational orientation) and are well illuminated. The user will need to manually add “tie-points” to the images if these conditions are not met.

The Seal Reader has different adapters for the Cobra Seal and the Quick Seal to accurately align the seals to the camera. These adapters provide a key feature for the automatic alignment of the seal images. The adapter for the Cobra Seal includes a conical housing and a key that the seal body slides into to orient the face of the seal in the same position each time the seal is placed in the Seal Reader. The images below represent two images from Cobra Seal 008 – applied and inspected.

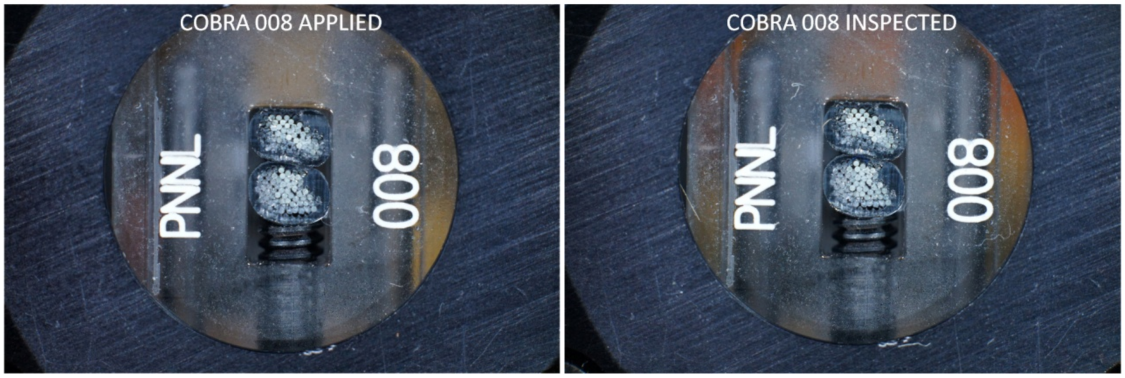

Figure 4 - Two images from Cobra Seal 008 (Applied and Inspected)

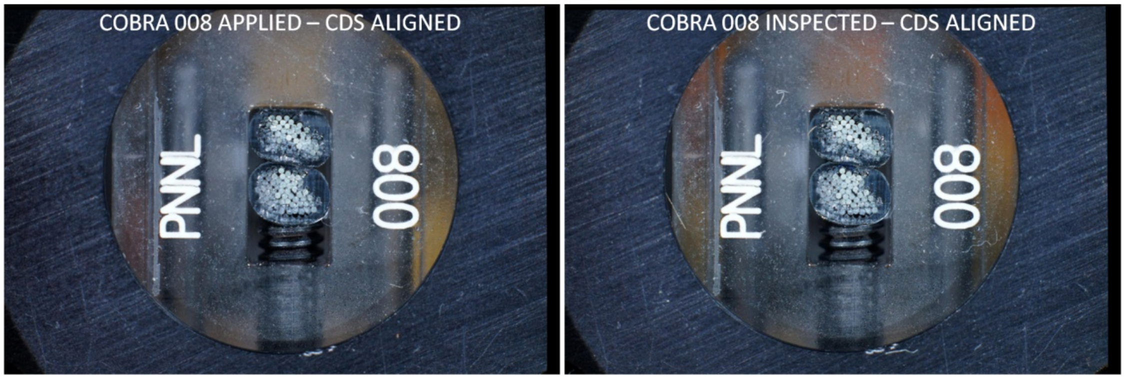
COBRA 008 APPLIED – CDS ALIGNED
PNNL
008
COBRA 008 INSPECTED – CDS ALIGNED
PNNL
008

Figure 5 - CDS aligned images of Cobra Seal 008

Double click Figure 6 to show the CDS aligned Cobra 008 images in a CDS type flicker display.

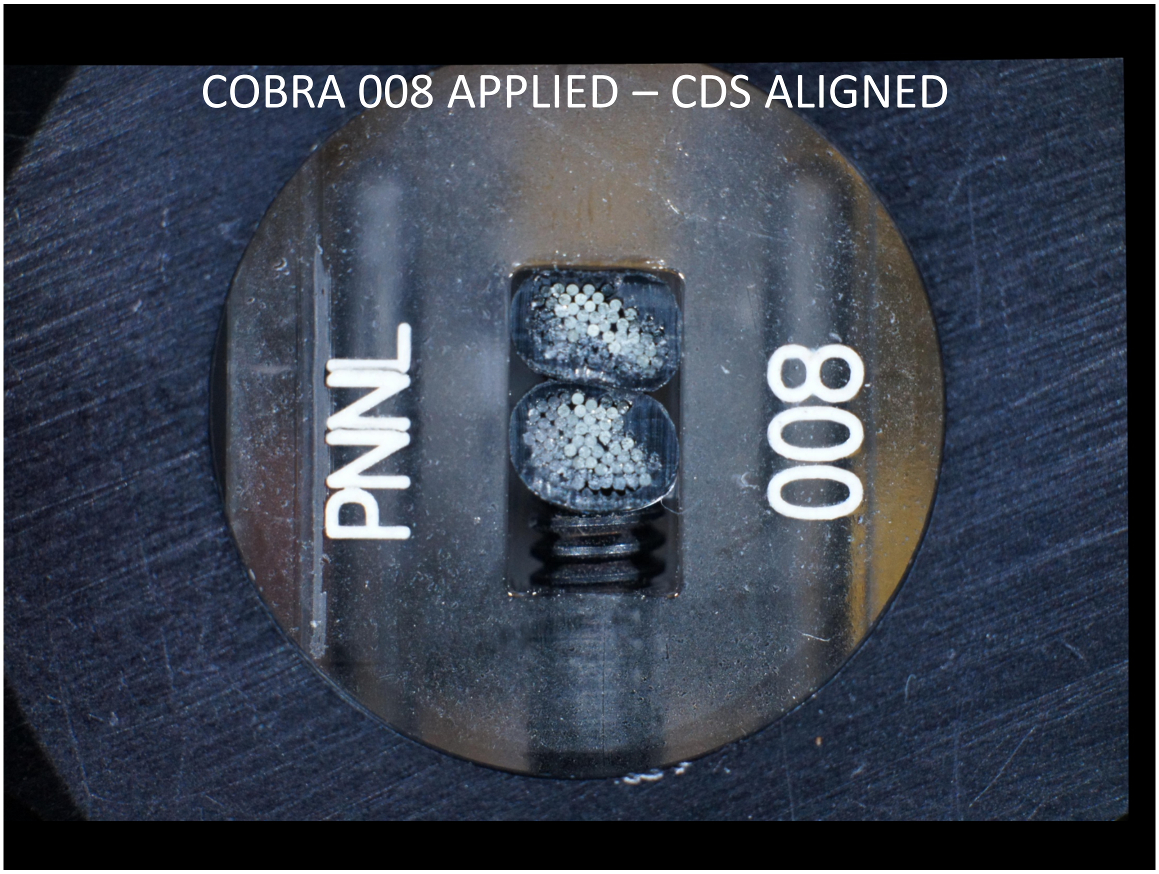

Figure 6 - CDS Aligned Images (Double click for flicker comparison)

The Seal Reader adapter for Quick Seals has slots that fit the outer dimensions of the seals. This provides for the placement and alignment of the seal in the reader assembly to provide images that can be rapidly aligned with CDS. All of the applied Quick Seal images have a more translucent appearance because the seal is not assembled when the applied images are taken.

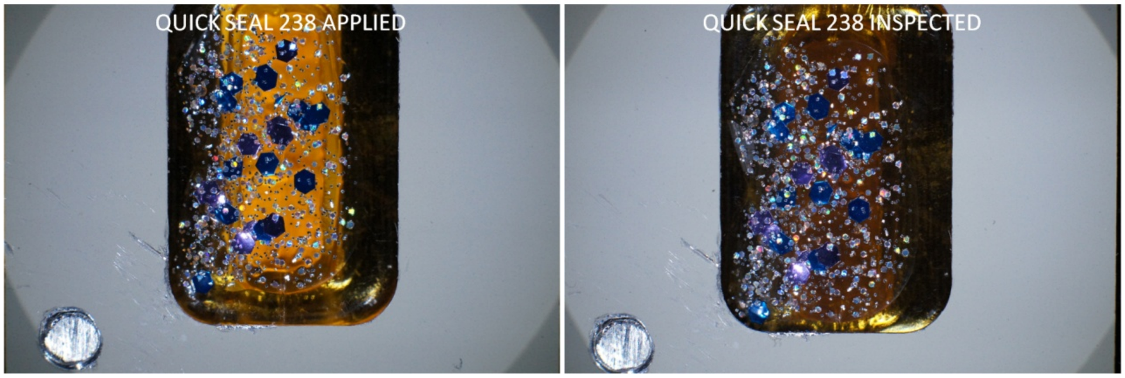

Figure 7 - Two images from QuickSeal (Applied and Inspected)

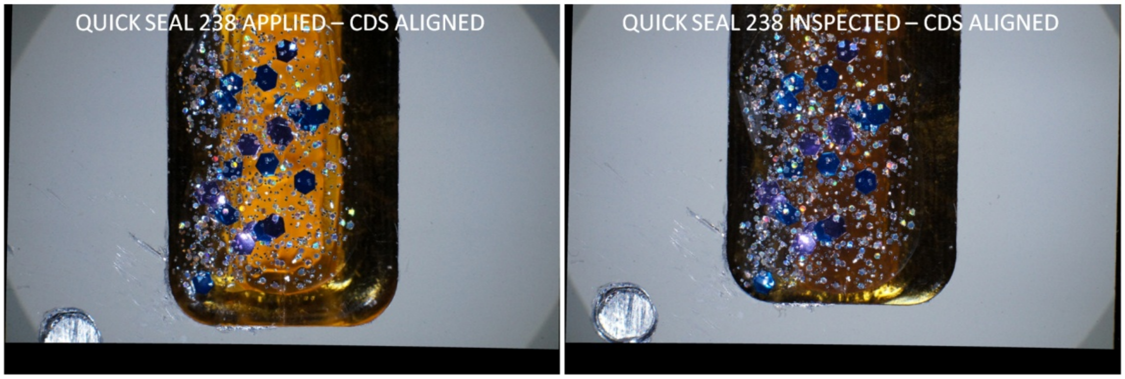
QUICK SEAL 238 APPLIED – CDS ALIGNED
QUICK SEAL 238 INSPECTED – CDS ALIGNED

Figure 8 - CDS aligned images of QuickSeal 238

Double click Figure 9 to show the CDS aligned Quick Seal 238 images in a CDS type flicker display.

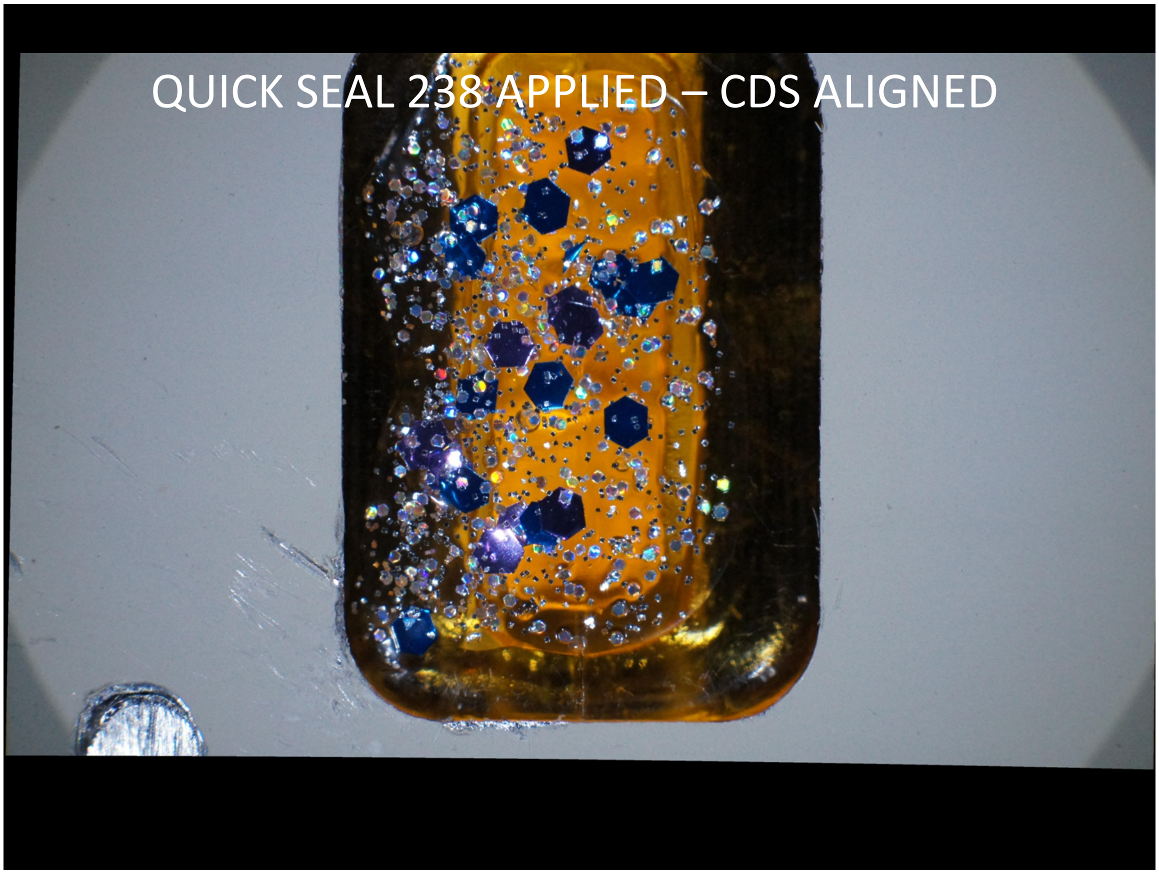

Figure 9 - CDS of Aligned Images (Double click for flicker comparison)

5. Authentication and Certification of Equipment

Before equipment can be used in a treaty verification scenario, the inspector must be assured that the equipment is authentic, and the facility operator must certify that the equipment meets his safety, security, and operational requirements. Meeting both authentication and certification requirements is extremely difficult. The host typically performs his certification testing without allowing the inspector to be present, and the inspector cannot apply many of the authentication procedures that he'd like to use because they would violate the host's certification.

Therefore, the equipment must be designed such that any attempt to modify the equipment during the host certification procedure must be easily detectable by the inspector during the on-site authentication process. Since this is often not possible, one or more copies of the equipment might be randomly selected by the inspector for further off-site inspection. If any tampering is detected during this off-site authentication, the equipment used during the inspection activities at the host's site would also be assumed to be compromised, and all data taken with that equipment would not be used for verification purposes. This would likely mean that the host would not be given credit for any treaty related activities in the effected period.

The design processes and authentication methods are beyond the scope of this paper and have been covered in some depth elsewhere[5].

6. Field Exercise Experience

6.1. ATL

The ATL was recently utilized in an international monitored weapons dismantlement exercise which took place in November 2011, and was one piece of an integrated chain of custody regime. The implementation of the ATL during the exercise turned out to be less than ideal. The main issue was due to the geometry of the room in which it was deployed. The ATL needed to be installed at a distance from the cameras where their pixel resolution was less than the width of one of the LEDs. This caused problems with the analysis software being able to resolve whether or not an individual light was on/off. Another issue which arose was driven by the adversarial nature of the exercise. The monitoring party had to worry about the host party attempting to subvert the chain of custody regime. In this case, the worry was that the host party might attempt to record the ATL signature from another camera, and send a false feed to the monitoring party recording devices. The way in which this was mitigated was to collimate the ATL LEDs to such a degree that it was impossible to read the ATL signature outside of the monitoring party's camera field-of-view (FOV). The unintended consequence was to make the installation and alignment of the ATL extremely difficult. A slight change in location or angle of the ATL resulted in a large change in the camera's FOV across the room.

The deployment of the ATL as part of the exercise provided significant first-hand experience which will help drive future design requirements. First and foremost, it highlighted the importance of utilizing digital format whenever possible. This allows for direct encryption and application of digital signatures. The lessons learned in the previous paragraph highlight the importance of understanding the environment in which future versions may be deployed. Having the ability to mount the ATL very near the camera would eliminate many of these issues; LED resolution, surreptitious recording of signal, and collimation of the signal.

[5] K. Tolk, "Hardware Authentication - Considerations and Approaches", *Proceedings of the 51st Annual INMM Meeting,* Baltimore, Maryland, July 2010.

The concept of an authentication tool for analog signals is extremely important. One success of the exercise was the lessons learned during the employment of the ATL as the best available solution to the analog signal authentication problem under the exercise constraints.

6.2. Seal Reader

The main tools for maintaining chain of custody over treaty accountable items are tags and seals. There are many variations to choose from, but the traits common to all successful tags and seals are the ability to detect unauthorized access to the item, and a unique identifier to provide confidence in the authenticity of the tag/seal. Additionally, the most common method of seal verification is through the use of photographs. When a seal is applied, a reference image is taken, and at each subsequent seal inspection another image is taken for comparison. In previous exercises, the images were taken free-hand which resulted in differing fields-of-view in many instances. Comparison of images then required each to be aligned to the reference through the use of change detection software. For large file sizes, this could take on the order of minutes. In the case of the exercise, over 100 tags/seals were deployed with multiple images taken of each. This would make comparison of every image impossible, which would introduce a severe vulnerability into the chain of custody regime. Therefore, a seal reader was fabricated with interchangeable fixtures to accommodate every seal type that was used in the exercise.

The seal reader was simple enough to use to where multiple host party members could easily pick up the device and take perfect images without the necessity of prior training. This significantly reduced the time required to install, verify, and recheck tags/seals throughout the entire exercise. This ability also increased confidence in the overall strength of the chain of custody regime. The alignment jigs on the reader made it possible to consistently align images to a degree where further preprocessing was not necessary prior to comparison with change detection software. Finally, the interchangeable heads allowed for one camera to be used for every seal image. This eliminated the need to acquire multiple identical cameras, lowering costs, or introduce uncertainties into the images through the use of different cameras with potentially varying resolution and image quality. The success of the seal reader during the exercise highlighted the importance of maximizing the usefulness and flexibility of available tools.

7. Future Development and Design Improvements

As discussed in section 6.1 above, the sensitivity of the ATL to position and alignment is a major issue for future development of this technology. Methods of protecting the ATL signature which don’t rely on collimation and alignment need to be explored. Several areas of exploration have been proposed, but no further work is ready for publication at this time. The major success of this first prototype was not that it worked flawlessly, but that it showed that authentication of analog video signals is possible.

The seal reader worked well during the field exercise, but there are several design improvements that would make the reader easier to use. The various adapters need to be optimized for the different seals. The connection of the adapters to the seal reader could also be made easier by using a quick release connection instead of the thumb screw. Also, the LED sequencing is slower than desired. This could be changed so that the process of imaging a seal is quicker and more efficient.

8. Conclusion

The ATL device and the Camera Seal Reader are examples of two pieces of equipment that have been designed, fabricated and field tested for use in a Chain of Custody regime. These devices were designed to aid arms control inspectors in performing containment and surveillance during a weapons dismantlement process. Design improvements have been identified to optimize these devices for potential field use in the future.