SAND--92-1676C

DE92 018820

Reflective Particle Technology for Identification of Critical Components*

Keith M. Tolk
Sandia National Laboratories
Albuquerque, NM 87185

ABSTRACT

Reflective Particle Tags were developed for uniquely identifying individual strategic weapons that would be counted in order to verify arms control treaties. These tags were designed to be secure from copying and transfer even after being left under the control of a very determined adversary for a number of years. This paper discusses how this technology can be applied in other applications requiring confidence that a piece of equipment, such as a seal or a component of a secure container, has not been replaced with a similar item. The hardware and software needed to implement this technology is discussed, and guidelines for the design of systems that rely on these or similar randomly formed features for security applications are presented. Substitution of identical components is one of the easiest ways to defeat security seals, secure containers, verification instrumentation, and similar equipment. This technology, when properly applied, provides a method to counter this defeat scenario. This paper presents a method for uniquely identifying critical security related equipment. Guidelines for implementing identification systems based on reflective particles or similar random features without compromising their intrinsic security are discussed.

INTRODUCTION

In order for international agreements and treaties to be effective, all involved parties must be confident that none of the parties can break the agreement or treaty without being detected. This is especially true in the case of treaties of long duration because the goals and objectives of the parties involved in the agreement can change significantly over the life of the treaty. The proper use of tagging technology can increase this confidence significantly and thereby tend to stabilize what could become a volatile situation. On the other hand, tagging or any other verification technology that is not properly applied can lead to a false feeling of security that could be disastrous in a changing political environment.

* This work was sponsored by the Bureau of Engraving and Printing, the Department of Energy, and the Defense Nuclear Agency.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

In order for a tagging system to provide its highest level of security, the tag and its verification technology must be included in the system engineering phase of the equipment to be tagged. Unfortunately, this is not a technology that can be placed on the shelf and applied without consideration of the entire verification system involved. Fortunately, the technology is well enough understood to allow this to be done rather easily in most cases.

SOME BASIC PRINCIPLES OF TAGGING

For convenience, any pattern used to identify an item shall be referred to as a tag in this paper. In general, a tag consists of a pattern that can be used for identification and a means for attaching that pattern to the item. By this definition tags include both applied tags that are applied to the surface of the item and intrinsic tags which are either a natural or added feature of the item.

Tags are applied to items to identify them as belonging to a specific group, to identify specific items, and to count items that can not be conveniently assembled into one area for counting. An example of the first use is the hologram applied to MasterCards and Visa cards to identify them as being authentic. The reflective particle patch on the seal body of the Python seal is and example of the second, and the reflective particle tag developed for counting strategic nuclear missiles is an application of the third. Actually, this last application is an example of all three uses. It identifies a piece of equipment as belonging to the group of legal missiles, it is associated with a specific item, and it is used to count the mobile missiles in the possession of one of the parties to a treaty.

Each of these applications have one requirement in common. Duplicating the tag must be beyond the capabilities of all potential adversaries in the time available.. In order to evaluate this, the potential adversary must first be analyzed. First, what is his motivation? This leads to the determination of how much he might be willing to spend to develop technology to duplicate the tag and how much he might be willing to spend to duplicate each tag. This can be as high as several million dollars per tag for some systems. Next, how much access will the adversary have? In applications where the items will be under constant, reliable supervision, a relatively simple tag will suffice. If the tagged item or the data required to duplicate the tag will be left in the hands of the adversary for a long period of time, a much more secure tagging technology is required.

Don Bauder, who originated this work at Sandia National Laboratories (SNL), developed four basic principles relating to duplication and counterfeiting of tags and similar items. First, any pattern made to a specified design can be duplicated using identical technology. This has been recently demonstrated in the counterfeit holograms on the credit cards coming from Hong Kong. Second, any surface feature can be duplicated. Although there is a limit to the level of detail that can be copied, this has been demonstrated to be true for all magnifications that are practical for field use. Third, any two dimensional pattern can be duplicated, no matter how complicated. Fourth, the most difficult pattern to copy is a multidimensional pattern produced by random processes. Reflective particle tagging technology is based on this principle and no practical process for copying a properly designed tag based on this technology has been demonstrated.

Another requirement for most tagging systems is that the tags must be secure from transferring to other, illegal items. This is especially true for systems used to identify specific items, such as seals and tamper indicating containers. The most secure article identification systems are based on features that are actually a part of the item to be identified. For example, if a tamper indicating container can be made in such a way that the material forms a random pattern in the body of the wall material, transfer would be virtually impossible. Since this is not always practical, especially if another party is making the item or if the item already exists. Using the adhesive that attaches the tag to the item as a part of the random pattern is almost as secure against transfer if the proper materials are used. This will be discussed in more detail later in this paper.

REFLECTIVE PARTICLE TAGGING TECHNOLOGY

A reflective particle tagging system consists of a tag applied to the item to be identified, a reader to record the reflective pattern information, a means of comparing the reflective particle information to prior readings of the same information, and other inspection equipment as required for the application.

The need for equipment to read the information and the need for a means of storing the data for comparison to subsequent readings are the main drawbacks to the use of random pattern technology. For applications that do not require the very high levels of security provided by this technology, other tags such as holograms that can be verified by simple inspection are preferable. However, for long term security, no other technology has proven to provide the level of security that reflective particles and other random patterns can provide.

Reflective particles are one of the simplest random patterns to use for identification because they are easy to apply and can be read using relatively simple equipment. The resulting patterns are very difficult to reproduce, since thousands of reflectors would need to be positioned very accurately by a prospective counterfeiter.

THE TAG

The tag, shown in figure 1, consists of reflective particles suspended in an adhesive matrix and other features required for aligning the reader to make the measurements and to identify the tag to simplify matching it to data taken on earlier readings. A protective overcoat may also be applied to protect the tag from environmental hazards. Each of these things that make up the tag must be chosen with care.

The reflective particle chosen for the treaty verification tag is a crushed crystalline material, micaceous hematite. This was chosen primarily because of the irregular shape of the particles. This gives a great deal of information that can be used for verification of the authenticity of the tag, and makes the potential counterfeiter's task much more difficult. Other particles, such as aluminized Mylar can be used in most applications in which the potential adversarial threat is not so extreme.

The adhesive is one of the most difficult items to choose. It must adhere to the surface to be tagged well enough that it will break up into small pieces if an adversary attempts to peel it off. It must be viscous enough to support the particles during application, and after curing it must be stable enough to prevent the particles from realigning themselves.

The requirements of the alignment features depend very strongly on the reader and image comparison techniques used. They must be stable enough to not fade or move during the useful life of the tag. They must be easy for the reader operator to detect to align the reader to within the tolerance allowed by the image comparison technique. In general, the reader position must be within about one millimeter of the position used for prior readings. If the alignment is much worse than this, the pattern of reflections changes significantly. In addition, these alignment features may need to be used in the image comparison process to minimize the time required for the software to align the images.

An environmental protective overcoat is optional and serves mainly to act as a moisture barrier and to give some protection from abrasion. If applied properly, it can also complicate counterfeiting and transfer attempts.

READERS AND IMAGE COMPARISON EQUIPMENT

The reader consists of lights to illuminate the reflectors from at least two lighting angles and some means of recording the resulting images. Readers have been built using instant print cameras, still video cameras, 35mm film cameras, and video cameras with various recording technologies. Each of these has its advantages and disadvantages. The best one to use depends on the application.

The instant print camera is relatively simple and easy to use, but is relatively slow since it must be realigned for each lighting angle used. The resulting prints can be compared with corresponding prints of earlier readings that the inspector brings with him. We have found that experienced operators can match these prints very reliably. They can't, however, detect the small variations that would be present in a carefully produced counterfeit. The images from these readers look like pictures taken of a starry sky, as shown in figure 2. The inspector can pick out the "constellations" in the prints, but he can't always tell if one of the "constellations" has moved slightly from one image to the next.

The still video camera is more convenient to use since the camera can be positioned once and the lights activated individually to take a picture at each of the required lighting angles. The images are stored on a small floppy disk. Unfortunately, extra equipment is required for the operator to know if he has gotten good images, and comparison of the current images to prior images is very difficult.

The 35mm camera is very similar in use to the still video camera. It has the advantage of much higher resolution. The film must be developed before the image quality can be verified and the images compared. This can be a significant liability in a treaty verification scenario in which the suspected illegal treaty limited item could be moved or replaced before a subsequent inspection.

Video cameras were used in the reader systems developed at SNL for treaty verification applications. One of these systems is shown in figure 3. This system consists of the remote reader, which contains the lights and camera, a control unit containing the power supplies and the removable hard disk used for recording the images, a recorder correlator unit containing the function keys and display and the digital computer, and a small video monitor for viewing the images and for use in aligning the reader. This system is portable and can operate over a wide temperature range. It has been tested to operate reliably from -20F to 125F. Several options are available for alternate configurations of this equipment and prototypes of some have been built. These can allow the operator more freedom if several tags are to be read at one facility.

The image comparison algorithm used with this type of system consists of three major steps. First, the reflector information must be extracted from the background information. This background information can be used as a secondary means of validation of the tag, but its presence can lead to errors in the comparing the reflective particle images if it is not removed. Second, the image from the current reading is aligned with the image from a prior reading. Third, the images are compared mathematically. These second and third steps are repeated until there is no further improvement.

The actual image comparison can be accomplished by calculating the classical correlation function or by doing a pixel-by-pixel subtraction of the two images and comparing the optical energy in the resulting difference image with the corresponding energy in the original images. This latter method is slightly easier to implement and is used at SNL.

OTHER INSPECTION EQUIPMENT

Additional inspection equipment may be required depending on the adversarial threat and the level of security required. The inspector must be able to verify that the tag is a valid tag. This requires verification that the reflectors are the proper size and shape and that they appear to be the proper material, that the reflections are coming from the reflective particles, that the tag appears to have been made by the proper process, and that the tag shows no evidence of tampering or transfer.

One of the most useful pieces of equipment for this purpose is a small, hand-held microscope. If subsequent review of the inspector's data is required, the images from the microscope are recorded either on film or using the computer. The images from the instant print camera and the 35mm camera usually have enough resolution to do this inspection without additional hardware.

If tags or seals can be removed at random for subsequent analysis at home, the field inspection process is greatly simplified. The threat of this analysis will deter most adversarial threats.

SUMMARY

Tags can provide a very high level of security for the identification of seals, secure containers, and other equipment for treaty verification and nuclear materials management. In order to be secure, the tag must not be able to be copied or transferred by any potential adversary.

Reflective particle tags provide the highest level of security of any tags now available. The additional cost and complexity of the equipment required for tag verification is easily justified in applications requiring the ultimate in security.

Reflective particle technology is mature and has had extensive testing and adversarial analysis. The tagging system should be customized to provide each application with the proper level of security. This can generally be done relatively easily.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

A. REFLECTIVE PARTICLE TAG

The Reflective Particle Tag is composed of micaceous hematite particles mixed into a clear plastic material (Figure 2). The mixture is painted onto the item to be identified. When the tag is observed using a small light source, the facets of the hematite particles that are in certain orientations will reflect the light to the observer, creating a pattern of bright spots. When the light is moved to another location, a completely different set of hematite facets will reflect, creating a different pattern of bright spots. Figure 3 is a typical image taken with a single light. Figure 4 is a picture of the same tag taken with a different light location. When the tag is read with several different light locations, the set of different images is a function of the random locations of the reflective particles and the random angles of their reflective surfaces. The shapes of individual hematite particles constitute another unique feature that can be used for positive identification if necessary (Figure 5).

REFLECTIVE PARTICLE TAG

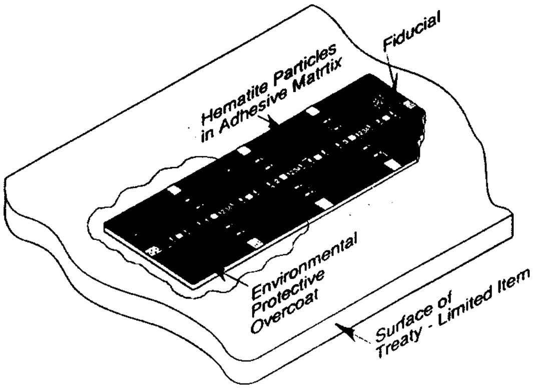
Hematite Particles in Adhesive Matrix
Fiducial
Environmental Protective Overcoat
Surface of Treaty - Limited Item

Figure 2. Reflective particle tag.

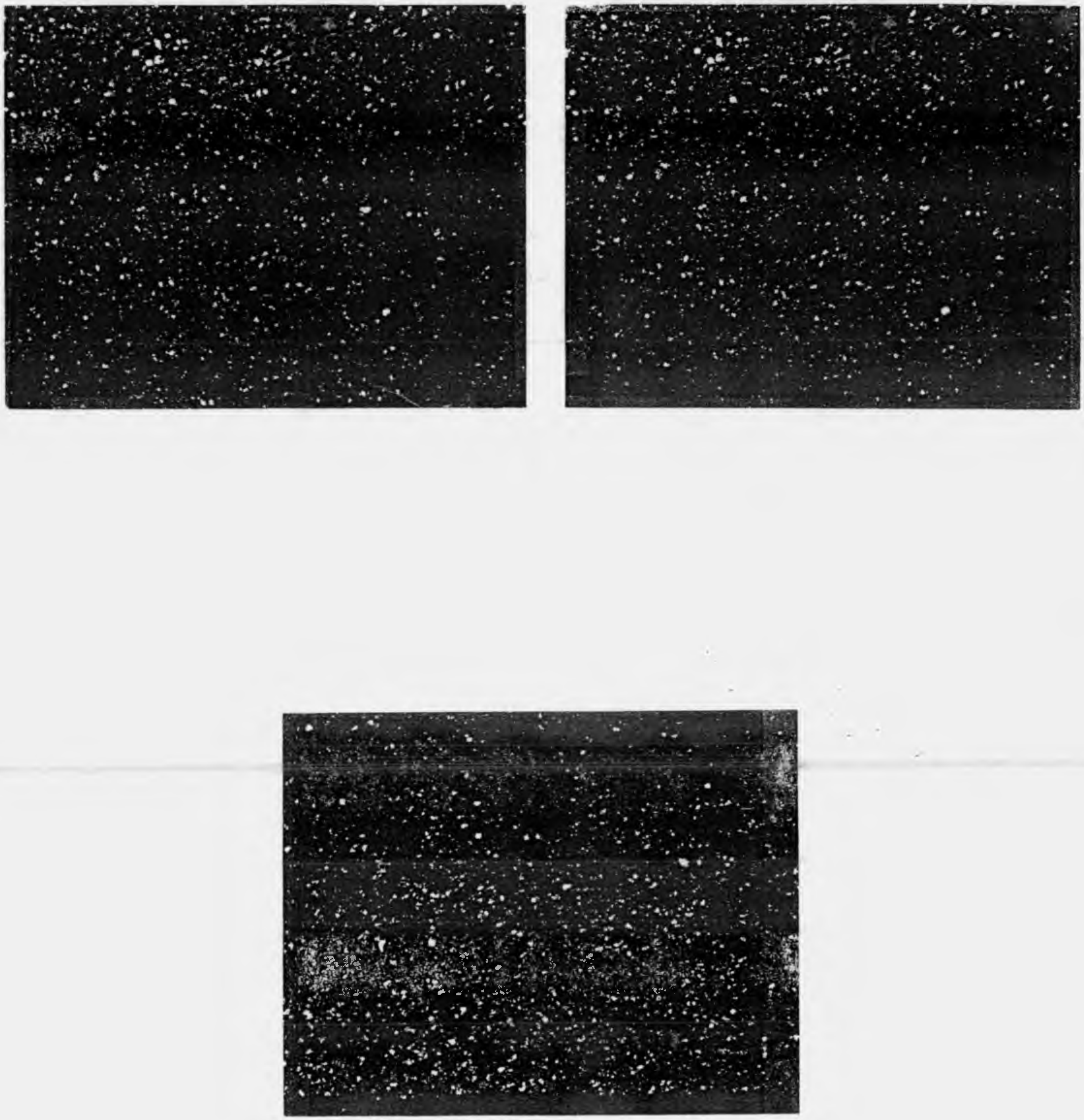

Figure ~~8~~ 2. Two images of the same tag and one image of a different tag.

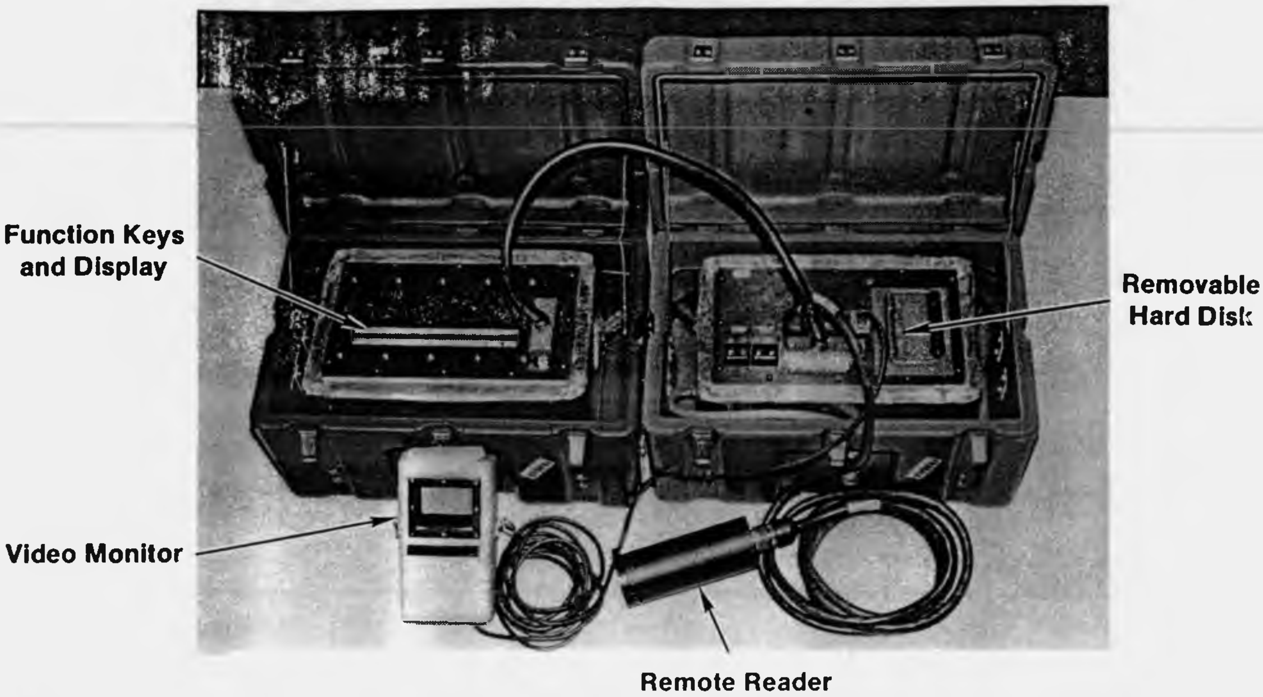

Figure ~~14~~ 3. *Remote Head tag reader system.*

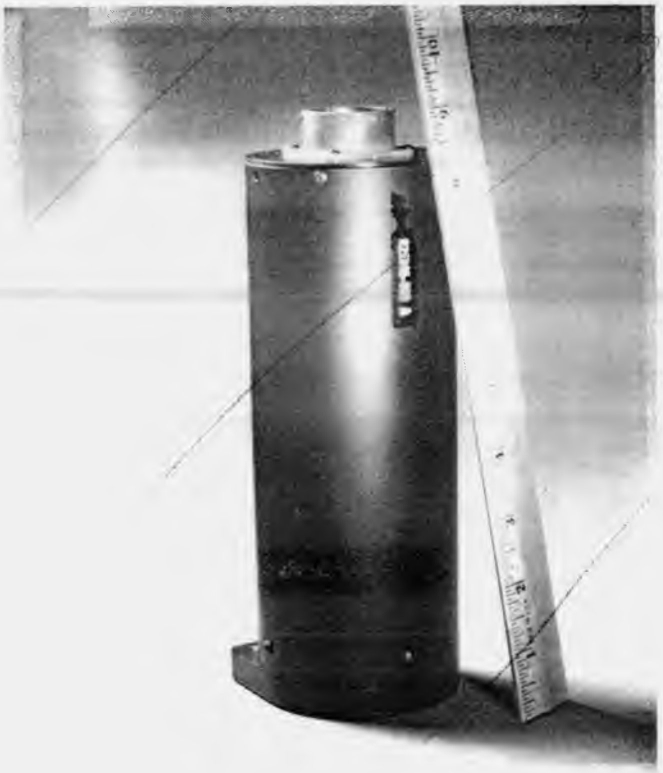

Figure 15. Remote head reader.