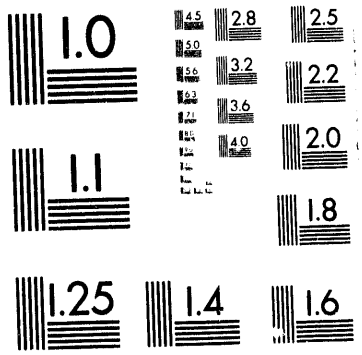
1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3

1 of 1

2

SAND--93-2470C

Conf-9404109--1

Random Patterns and Biometrics for Counterfeit Deterrence*

Keith M. Tolk
Sandia National Laboratories

Abstract

Sandia National Laboratories (SNL) has been working on non-counterfeitable seals, tags, and documents for over fifteen years. During that time, several technologies have been developed that can be applied to deter counterfeiting of identification documents such as ID cards, passports, and possibly credit cards.

Two technologies are presented in some detail. The first is reflective particle tagging technology that was developed to help verify treaties limiting the numbers of nuclear weapons that participating parties may possess. This approach uses the random locations and orientations of reflective particles applied to the surface of an item to uniquely identify the item. The resulting tags are secure against even the most determined adversaries. The second technology uses biometric information printed on the document and public key cryptography[1] to ensure that an adversary cannot issue identification documents to unauthorized individuals.

Executive Summary

Random pattern technology developed for the verification of nuclear arms control treaties can be used to protect security badges, credit cards, currency[2], and other documents from even the most determined professional counterfeiters. The price for this increased security is the need for a reader/authenticator device at every point that the authenticity of the documents must be proven. A considerable increase in the amount of data stored on the documents is also required. Whether the increased cost and complexity are justified in order to obtain the increased security must be determined for each potential application. As the costs of the electronics required for the reader/authenticator continue to decrease, this approach will be economically attractive for more applications.

A randomly produced feature is added to or identified on each type of document to be protected. Data describing this feature and other identifying information such as the authorized user's name, account number, and biometric data are recorded on the document. A data signature produced using public-key data authentication is also stored on the document. When the document is presented for use, the authentication signature is verified to be appropriate for the data file on the document using one of a set of public keys corresponding to the set of authorized issuing stations. This verifies that the data has not been tampered with and that the document was issued by an authorized issuing station. Then the pattern is read and compared to the data file to verify that the pattern has not been altered. The authenticity of any other identifying data is also verified at this time. If all of these tests are passed, the document is known to be authentic and unaltered.

* The work reported here was made possible by Sandia National Laboratories' Laboratory Directed Research and Development (LDRD) funding. Prior work by the author in related areas was funded by the Bureau of Engraving and Printing, the Department of Energy, and the Defense Nuclear Agency.

Biometric data can also be considered to be a special case of a randomly produced pattern. When biometric data is used in this application, it also serves to tie the credential to the authorized user. Information derived from the photograph or fingerprint printed on the document works well for this type of application. The photograph has the added advantage that a human can do a pretty good job of comparing the photograph to the individual without the need for additional equipment. If more security is required, other biometric information such as hand geometry or retinal scan can be included and verified using appropriate hardware.

Introduction

One of the first steps in designing a counterfeit deterrence system should be to analyze the level of sophistication and the motivation of the expected adversaries. For example, if we are concerned about counterfeiting of hundred dollar bills, we only need to make the system secure enough to force a potential adversary to spend more than one hundred dollars to make each bill in order to make the enterprise economically unattractive. In fact, a cost of ten percent of the face value is probably adequate to deter most counterfeiters.

Many system designers tend to underestimate the sophistication and motivation of our adversaries. For that reason, we tend to design counterfeit deterrence systems with the highly motivated, very sophisticated adversary in mind. It is often easier to make a system less secure and therefore less expensive than to add security to a basically flawed system. One reason that we approach the problem in this manner is that most of the applications that we have been involved with have been concerned with very determined, very well funded adversaries, such as foreign governments. These adversaries might be willing to spend millions of dollars on counterfeiting equipment. In one instance, it was estimated that the adversary might be willing to spend over a million dollars to make a single counterfeit. While most systems do not need to address such determined adversaries, many of the same principles can be applied to less demanding applications.

Don Bauder, who originated this work at SNL in the late '70's, developed the following four basic principles relating to duplication and counterfeiting of tags and similar items:

- Any pattern made to a specified design can be duplicated using identical technology. If I am willing to buy the same equipment that was used to make the original, I can probably make an exact duplicate. The basic axiom is "What one man can make, another can copy."[3]

- 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.

- Any two dimensional pattern can be duplicated, no matter how complicated.

- The most difficult pattern to copy is a multidimensional pattern produced by random processes. Reflective particle tagging technology[4] is based on this principle and no practical process for copying a properly designed tag based on this technology has been demonstrated.

Random Pattern Basics

Random patterns are used for counterfeit deterrence by reading descriptive data from the pattern and comparing it to similar data taken earlier, usually at the time the document was issued. The following components are required for a random pattern system:

- A suitable random pattern

- A reader system for reading descriptive data from the pattern
- A means for storing the data for comparison to the pattern on subsequent readings
- A means for comparing the data sets to determine if the pattern is authentic.

In order for a pattern to be considered for this type of application it must satisfy the following criteria:

- Stability - It must be not change over its useful life when exposed to the most severe of its expected environmental conditions.
- Readability - A reader system must be designed to read descriptive data from the pattern.
- Non Duplicability - The pattern must not be duplicable by any practical means.
- Uniqueness - All patterns generated by the process must be different enough from each other that a randomly produced copy cannot be confused with the original pattern.

Several different reader systems are possible, depending on the random pattern used. For optically readable patterns, film cameras, still video cameras, and video cameras are available. For magnetic patterns, read heads similar to those used in magnetic stripe readers are used.

Data storage can be accomplished using various forms of digital storage or the analog waveforms can be recorded. The data can be stored at a central site and transmitted or carried to the verification site, or the data can be stored on or with the item to be authenticated by using encryption or authentication techniques. The latter method is the most attractive for use on currency, credit cards, and identification cards.

Some form of correlation calculation is generally used for comparing the data sets to verify authenticity.[5]

The need for equipment to read the information and the need for a means of storing the data for comparison to prior readings are the main drawbacks to the use of random pattern technology. 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.

Other random patterns that may be of interest include the shape and location of special fibers added to paper during the manufacturing process, the random timing errors that occur in recording magnetic stripe information[6], and biometric information. Biometric information is generated by an individual's genetic patterns and can also be thought of as random patterns. Biometric data printed on an identification document can be used not only to verify the authenticity of the document, but can also tie that document to the person authorized to use it. This is the basis of the second application that will be discussed later in this paper.

Reflective Particle Tagging Technology

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 or similar technology might be useful for deterring the counterfeiting of credit cards or other, similar documents.

The tag consists of reflective particles suspended in an adhesive matrix applied to the surface of the item to be identified. The reflective particle chosen for the treaty verification tag is a crushed crystalline material, micaceous hematite. This was chosen primarily because of the irregular size and shape of the particles. The particles also tend to orient themselves more randomly than other reflectors, such as aluminized Mylar. 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 reader for the reflective particle tag 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 simple and easy to use, but is relatively slow since it must be adjusted for each lighting angle used. The resulting prints can be compared with corresponding prints of earlier readings that the inspector has made and brings with him. We have found that experienced operators can match these prints very reliably. They cannot, however, detect the small variations that would be present in a carefully produced counterfeit. The images from these readers look like pictures of a starry sky. The inspector can pick out the "constellations" in the prints, but he cannot 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 specified 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. However, 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. The system is portable and can operate over a wide temperature range for outdoor use. 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. Most of these 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 two original images. This latter method is slightly easier to implement and is used at SNL.

Reflective Particle Technology for Cards and Other Documents

Reflective particles can be laminated into a multi-layer card such as a credit card or an identification card. These can be read with a fairly simple reader consisting of a video camera, two or more LED's to provide lighting, and a simple computer with a frame grabber. Such a reader can be built today for $1500 to $2000 using commercially available hardware. This cost could be reduced if the reader is produced in large enough quantities.

Over 250 kilobytes of data were stored for each reflective particle tag in the treaty verification application. Since the expected counterfeiter for cards, currency, and other documents is much less sophisticated and much less motivated than that expected in a treaty violation scenario, this can be reduced considerably. The desired amount of stored data is related to the difficulty of copying the pattern.

The issues of data storage and data authentication are similar to those encountered in the use of biometric data and will be discussed later in this paper.

Use of Biometric Data on Identification Cards

The application can best be illustrated by use of an example. Consider the security badges issued by Sandia and other DOE laboratories. The main features of the badge are a picture of the individual, his or her name, any special access information, and a printed substrate to identify the issuing agency. These items are laminated to prevent damage and to deter an adversary from making changes. In the proposed system, additional information would be included with the badge in authenticated form. This information would include the person's name, a control number, access authorization information, and authentication information for the photograph on the badge. When the individual presents the badge for access to a facility, it is placed into a reader that scans the photograph and reads the authenticated information. The information is verified using one of a table of public keys. The authenticated information would be compared to the photograph, using algorithms similar to those we developed for the reflective particle tagging project, to verify that this is the photograph that was on the badge when it was issued. The reader would also compare the control number to a list of lost, stolen, and revoked badges. On the basis of this information, the reader would then make a decision on the authenticity of the badge. This authentication process will probably take on the order of five seconds using relatively inexpensive computing equipment. The reader would then display the person's name, his security clearance level, and whether or not he is currently authorized access to the facility. The guard or access control officer then decides if the individual is the person pictured on the badge and grants or denies access.

Note that this system does not preclude an adversary from making copies of an authorized badge. The copied badge will be difficult to use, however, unless an individual who strongly resembles the picture on the badge can be found to use it. If this is an unacceptable risk in the security system, other biometric information for the individual can be included in the data file and verified using appropriate technology.

The resulting system provides a robust, secure system that could include many locations without the need for a large database of issued badges. The only databases required are the control numbers of badges (or passports, etc.) that have been canceled by the issuing party and the public keys associated with authorized issuing stations.

Data Authentication and Key Control

In public-key data authentication, both a public key and a private key are used. The private key is used to generate unique signatures for data files and is known only at the data source and is not released to the public. The corresponding public key is provided to all users who must validate the signature for the data files[7].

This is an excellent application for public key data authentication. The method that we are implementing for the prototype application is the Digital Signature Standard (DSS)[8]. The private keys used to generate the data signatures in the issuing process could be generated using random events and will be stored only in the computers that issue the badges. Each issuing computer would have its own private key and would only reveal its public key to be distributed to the verification stations. No human would ever have to have access to a private key. These computers could be sealed units and would be kept in secure locations. The chip containing the key could also be protected with a special security coating.

The badge readers only need to be secured to a level sufficient to ensure that unauthorized public keys have not been added to its key table. This should be relatively easy to accomplish using data authentication techniques similar to those used for the data storage.

Data Storage

This is a trade-off between cost and technical difficulty. The least expensive form of storage for the authentication data on the document is to print the information using a two-dimensional code similar to Code 1 or PDF-417[9]. The total data storage requirement, when coupled with the small area available and the available printing technology, does not allow these existing technologies to be used directly. We are therefore developing our own two-dimensional code for this application. Using this type of data storage technology allows us to produce badges that are not significantly more expensive than those in use today.

If chip card technology is used, the cost of the cards increases, but the cost of the reader is reduced slightly.

Conclusions

Biometrics and other random patterns combined with public key data authentication can be used to increase the security of identification cards, passports, and other similar documents when the cost of this increased security is justified by the potential cost of counterfeits. As the cost of the authentication equipment continues to decrease, more applications will become cost effective.

References

[1] T. J. Draelos and S. Y. Goldsmith, "Public-Key Data Authentication for Treaty Verification," *Proceedings of the 33rd INMM Annual Meeting,* Orlando, Florida, 1992, pp. 959-964.
[2] *Counterfeit Deterrent Features for the Next-Generation Currency Design*, National Research Council, National Academy Press, Publication NMAB-472, 1993, pp. 74-75.
[3] ibid., p. 14.

[4] K. M. Tolk, "Reflective Particle Technology for Identification of Critical Items," *Proceedings of the 33rd INMM Annual Meeting,* Orlando, Florida, 1992, pp. 648-652.
[5] ibid.
[6] D. Jeffreys, XTEC Incorporated, personal communication, October, 1992.
[7] Draelos, et al., op. cit.
[8] "Specifications for a Digital Signature Standard," *Federal Information Processing Standards Publication XX,* National Institute of Standards and Technology, August 19, 1991.
[9] "Two-Dimensional Bar Code Symbologies," *Scan-Tech 91 Proceedings,* Dallas, Texas, 1991, Session 3D.

DATE
FILMED
4/6/94
END