To See Truth

Signa2

A brief description of a method for the indigenous authentication of digital information as described in US Patent 6,757,828 B1 of June 29, 2004.

Contact

Dr. Joel Goldhar, President
Goldhar/Jaffe Technology Development Corporation, Inc.
720 Foxdale Avenue
Winnetka, Illinois 60093
847-501-2552 voice
847-501-4074 facsimile
847-372-6631 mobile
goldhar@stuart.iit.edu

The patent may be downloaded from www.gjtdc.com

Why Digital Authentication Is Important

One major reason behind the shift from chemical to digital imaging and from paper and ink to digital files is the demonstrated ease with which information can be managed. Replacing paper and ink archives with digital files dramatically reduces the cost of capturing, analyzing, using, moving and storing information. Concern for the long term fragility and security of physically manifested information are also reduced. Ease of use is enhanced. As an example, for photography the cycle time from image capture to finished product rivals instant photography.

Unfortunately the same technology makes it very easy to covertly alter the information in a digital file. Users who must *authenticate* their information have special concerns when using digital information and imaging systems because of the wide availability of software for manipulating digital information that may leave little or no evidence of tampering.

Even physical manifestations are difficult, sometimes impossible; to authenticate. Consider the long history of art forgeries, the best of which remain undetected to this day. Any manifestation which contains only physical elements can only be authenticated based on those physical elements. For artwork, forgeries are detected based on materials inconsistent with those in use at the time as well as discrepancies in the form or style used by the artist. Even artwork with appropriate materials and style often cannot be conclusively authenticated as an unknown work of a famous artist.

An Early Solution

Others have developed the concept of a camera creating an encrypted image. The security of the image was protected by reverse encryption. The encryption key was tightly held inside the camera. There were certain fail safe devices that destroyed the key if someone tampered with the camera. As the camera was subject to accidental damage an alternative trusted source for the key pairs was created in the form of a key repository. This was later changed to a repository for decryption keys only. The only source for the encryption key was the camera itself.

Our Improved Solution - Signa2

We expanded the general case of detecting and correcting changes to digital files from either unintentional modification (such as transmission error or storage degradation) or intentional modification (such as an intent to deceive or virus infection). Tamper detection and fail safes were retained and enhanced. This new solution is called Signa2, short for signature, and uses digital signatures. A patent was granted June 29, 2004 and a proof of concept model was created using off the shelf components instead of application specific elements. The patent may be downloaded from http://www.gjtdc.com/

Signa2 Explained

Sensors and recorders, such as digital cameras, scanners, audio recorders, video recorders, chemical process sensors etc. are equipped with embedded processors and peripheral elements to create a file, or other recording, that can be validated as authentic (unaltered) from the point of recording. The validation program is widely available from a secure source and will report post capture alterations and optionally attempt to recover the original material from modified material. Additional inputs can be made part of the recording and validated as authentic and unaltered from the point of recording.

This authenticating system creates a digital signature unique to the recording and requires neither comparison files, conventional encryption, nor reverse encryption. The strength of the signature is increased by using one-time random elements as part of the signature creation. The strength of the signature can be increased further by the use of a random string, regenerated under user control. Although not required for basic operation the resulting recording can be optionally encrypted to conceal the information. The absence of required conventional encryption or reverse encryption eliminates the need for a public registrar or record keeping relating to the management of decryption keys. As the authentication is indigenous there is no requirement to know which recorder captured the information.

Properly embedded, this system can be used in any sensor-recorder system such as a digital still camera, digital video camera, digital audio recorders, digital telephones, and sensors for the entire spectrum of chemical, physical, mechanical, photonic, spectral and biological phenomena.

As an additional benefit, digital files can contain more than the elements needed to create an image. Additional authentication information may be generated indigenous to, and inseparable from, the capture device. These “tightly coupled” sensor-recorder systems provide for a high degree of reliability. While Signa2 cannot prevent fraud prior to capture, it can detect intentional or unintentional post capture alterations. If there are no alterations the image is authenticated as to accurately reproduce what was initially captured by the sensor-recorder. If there are alterations detected, Signa2 provides, in some situations, optional recovery capabilities to restore the image right down to a single picture element.

Signa2 also provides benefits in an arena where images need to be captured by potentially unreliable personnel. Concerns about the authenticity of an image can be materially reduced. With built in geo-positioning system and other options there is indigenous authentication of date, time and location of image capture.

Signa2 indigenous authentication technology provides not only authentication value, it also allows users who must guarantee the authenticity of their images or data to enjoy the cost savings and ease of use of digital information systems and technology.

Signa2 Devices

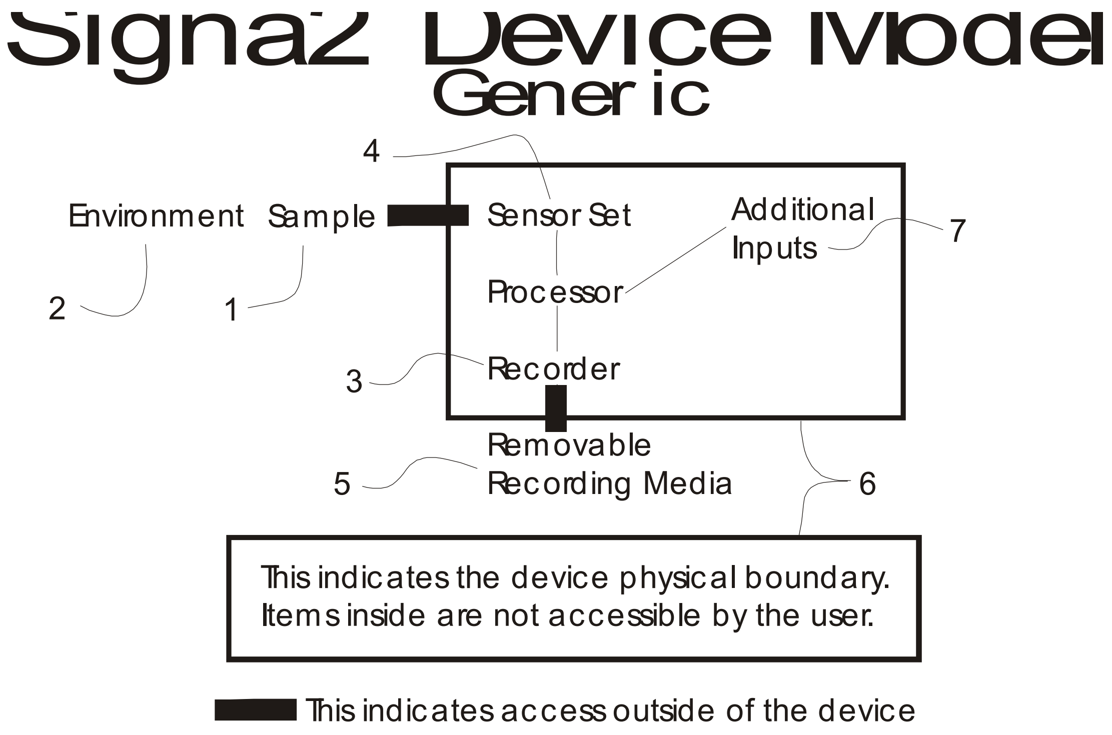
(see Figure 1 "Signa2 Device Model - Generic")

The purpose of Signa2 devices is to acquire and record a sample ***1*** *of the environment* ***2*** *in such a manner that the stored recording* ***5*** *is verifiable as an authentic representation of the sample* ***1*** *and has not been altered from point of acquisition in the environment* ***2****. Authentication information generation capability must be indigenous* ***6*** *to, and inseparable from, the device.*

Tightly Coupled - The key to verifiable authenticity is to insure that the signature generation is tightly coupled **6** to the sensor set **4** and recorder **3**. There is nothing that can alter the recording **5** created by the recorder **3**. The signature, as well as other data, is embedded in the recording. The authentication program can extract the provided signature and create a signature for comparison from the recorded sample.

Additional inputs **7**, those inputs other than the sensor set **4**, must be not accessible by the user or subject to tampering without detection. Thus, additional inputs are shown inside the device physical boundary **6**. Analog recorders can be accommodated for authentication by the inclusion of an analog to digital converter.

Figure 1


Signa2 Device Model
Generic
4
Environment
Sample
Sensor Set
Additional Inputs
7
2
1
Processor
3
Recorder
Removable Recording Media
5
6
This indicates the device physical boundary. Items inside are not accessible by the user.
This indicates access outside of the device

The generic Signa2 device model can be expanded and applied to any of the tight sensor-recorder couplings that are the desired arena for the Signa2 devices.

To record a single sample of a visual environment we would use a single frame optical recorder, a camera. The sample is known as a "photograph" and has been traditionally recorded on positive transparency films (slides), negative transparency films (negatives), opaque or translucent prints; and more recently as digital files.

Some uses for Signa2 authenticated images would include automatic images taken of toll and traffic violators, crime scene images, or any situation where chain of custody and reliability are material considerations.

Another major application is in authenticating reproduced material. Consider recently enacted *Check Clearing for the 21st Century Act* (Check 21). Reproduced substitute checks that have the legal stature of a canceled check beg for authentication. Another reproduction related application is in the area of document management. Given the increased requirements for records retention, in part due to the *Public Company Accounting and Investor Protection Act* (Sarbanes-Oxley), the amount of information, both paper based and electronic, required to be retained has grown mountainous. If the paper based information was scanned in a Signa2 enhanced scanner, it could achieve the same status as a substitute check. The paper is recycled, the substitute is stored electronically at a material and continuing cost savings. Without such an authentication indigenous to the electronic version what is to detect an alteration of the electronically archived element?

To record a continuous sample of a visual environment we would use a continuous optical recorder such as a digital movie camera. Such samples are generically called "movies" and have been recorded on transparency film, videotape and more recently as digital files.

To record a sample of an auditory environment we would use a continuous digital audio recorder. Such samples are called "recordings" and have been recorded on a wide variety of wire, tape and more recently as digital files.

Recording samples of taste, touch and smell can be accommodated in the same generic model as sensors and recorders are further developed and refined.

Samples are not limited to the five human senses. Samples can be taken from any sensor set including, but not limited to, the full range of chemical, physical, mechanical, photonic, spectral and biological phenomena.

The generic process of authentication is to acquire the original signature from the recording file, generate a new signature from the recording and compare the two. If the two signatures match then the recording is considered valid or authentic. Remember: in this document "recording" refers to all recordings, not only the more common audio or video recording.

Signa2 Distinguished

What distinguishes Signa2 from simply applying a conventional digital signature post-capture is the tight coupling of the sensor-recorder set, the provision for many elements of authenticateable optional data, the use of one time and random elements to effectively preclude reverse engineering of signature protocols, optional addition of encryption to increase security, detection of intentional or unintentional post capture alterations, and optional recovery capabilities down to a single picture element.

For additional information on legal aspects, technical notes on operations, the potential for a “diluted” version, conventional and reverse encryption, digital signatures, watermarking, random string, and probability, please see the addenda following.

Notes on Legal Concerns Using Digital Imagery as Evidence

1997-1998 House of Lords Report, Select Committee on Science and Technology

Digital images are admissible as evidence (altered or not) but their evidentiary value will be swayed by authentication and a secure audit trail from initial image to what is provided to the court. The recommendations of the House of Lords report emphasizes the need for secure audit trails from initial recording to copies produced as evidence. To this end, the indigenous nature of a Signa2 image has no equal. It is its own audit report.

The full report is entitled;
House of Lords, session 1997-98, 5th report
Select Committee on Science and Technology
Digital Images as Evidence

and is available from;
The Stationary Office, London
Telephone, 0345 023474
Reference HL paper 64

October 2000 United States Department of Justice / Federal Bureau of Investigation

Forensic Science Communications
October 2000 Volume 2 Number 4

Legal Ramifications of
Digital Imaging in Law Enforcement

"More and more agencies are choosing digital capture systems to eliminate the need for film-based imaging systems. The potential for budgetary savings and the ability to deliver images faster continue to drive more law enforcement agencies toward a conversion to digital imaging. Rapid moves toward any technology, without adequate research and planning, or the training needed to demonstrate competency and proficiency, can leave an agency vulnerable to misinformation and legal challenges." (from the Introduction)

This report echoes the concerns of the House of Lords regarding chain of custody as protection that the evidence is the same when it is presented as when it was acquired.

This report is available on line at
http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/berg.htm

April 2004 United States Department of Justice / Office of Justice Programs
National Institute of Justice
Special Report
Forensic Examination of Digital Evidence
A Guide for Law Enforcement

This guide shows the depth and breadth of suggested activities as part of the examination and control of digital evidence to assure that the evidence is unaltered from crime scene to courtroom.

This report is the second in a series. The first was *Electronic Crime Scene Investigation: A Guide for First Responders* available on line via http://www.ojp.usdoj. gov/nij/pubs-sum/187736.htm. All of the reports should be available on line via http://www.ojp.usdoj.gov/nij

July 22, 2004 New York Times
"For Doctored Photos, a New Flavor of Digital Truth Serum"
Noah Shachtman

This article starts out how a man, arrested in 2002 on charges of child pornography, was acquitted because the explicit pictures found on his hard drive could not be authenticated as original or forgeries. The man was eventually convicted on separate charges and sentenced to life in prison.

The article goes on to describe several projects underway to determine, post-capture, whether images are authentic. Signa2 is a proactive solution to the problem.

The article is available on line at www.nytimes.com, subscription required.
http://tech2.nytimes.com/mem/technology/techreview.html?oref=login&res=9806EEDE1E3AF931A15754C0A9629C8B63

Technical Note on the Operational & Authentication Sequence for Digital Signatures

The operational and authentication sequence runs this way

I take the picture (or capture a sample using another sensor set/device),
Create the signature
Sending you both picture and signature in a single file

You receive the single file
Generate the MD5 (or other) signature protocol using an authenticator program
Compare the generated signature to the one provided

If they match, then the picture (or other digital file) is as it was originally captured and is authentic.

Notes on a Diluted Variation

There are situations where authentication does not have as high a priority as does getting additional information native to an image. In the “diluted” version the security is not perfect, but "pretty good". These would be low cost enhancements added to existing devices. The security barrier isn't there, but everything else is, such as GPS, data/time stamping, unit identification, additional error correction, etc.

Notes on Conventional Encryption and Key Pairs

The original purpose of encryption is to reveal the true message only to the intended recipient. This is "restricted to receiver". A *key-pair* is created. That is one encryption key and one decryption key. The mechanics of modern encryption algorithms differ but each key in a pair work only with each other. That is a message encrypted with encryption key #1 (EK1) can only be decrypted by decryption key #1 (DK1).

Normally the encryption (sometimes called public) key is widely available and the decryption (sometimes called private) key is tightly held. So a sender of encrypted messages to many people would need many differing encryption keys.

For example: if a stockbroker wanted to send a coded message to a client:

- the message would first be created in plain text, then
- encrypted using the widely held client specific encryption key, then
- transmitted to the client, then
- decrypted by the client using the tightly held decryption key

While a message can be encrypted with DK1 (a decryption key) the message cannot then be successfully decrypted with EK1 (an encryption key). This is important because in both conventional and reverse encryption below one of the two keys must be tightly held. If you were able to successfully use the keys in the improper sequence the security would be compromised.

Notes on Reverse Encryption

Using the same basic concept in reverse we make readily available the decryption key but tightly hold the encryption key. Because the keys are paired if the file decrypts with decryption key then it must have been encrypted with the matching encryption key. This is "authenticated from sender".

So if I wanted to send a message that could only have come from me:

- the message would first be created in plain text, then
- encrypted using the tightly held encryption key (EK2), then
- transmitted to recipient, then
- decrypted by recipient using the widely held decryption key (DK2)

Since the message (or file or any digital source) is decrypted using DK2 then it could only have been encrypted using EK2. Unless the EK2 key was compromised (stolen or otherwise no longer tightly held) then the message was from the DK2 holder and is authentic. As the number of users increases, key management becomes burdensome.

Notes on the Digital Signature

According to www.Dictionery.Com a signature is . A distinctive mark, characteristic, or sound indicating identity: and signature \Sig"na*ture\, n. [F. (cf. It. signatura, segnatura, Sp. & LL. signatura), from the Latin signare, signatum. 1. A sign, stamp, or mark impressed, as by a seal. Consider a well known example of an early signature.

Clearly this was the signature of the first president of the Continental Congress, perhaps the most widely recognized signature in the history of the United States. No one else made such a mark. From a veracity point of view the drawback of this signature is that it is unrelated to the document signed. It would be the same signature on the Declaration of Independence or the bar bill at Tun Tavern. Even in 1776 an unauthorized individual could manually replicate the signature. This is called *forgery*. More than 200 years later such physical, non-adaptive, signatures can be digitized and reproduced. There are plotters that manipulate quill pens and can create signatures authentic to variable line width and differing pressure capable of creating thousands of "original" signatures.

Consider an adaptive, electronic signature. Here *adaptive* means that the signature changes depending on the material being signed. Electronic means that the signature is not a pattern of lines on paper, but bits in an electronic file. How the electronic signature is created is a function of the signature creation algorithm and the content of the file to be signed. **Is a representation of an environmental sample authentic, or has it been modified?** *If you can't tell therein lies the problem we're trying to solve.*

A Comment on Watermarking

Watermarking is a concept designed to clearly and continuously identify the owner, but not necessarily the sender, of an image or document. It has nothing to do with the authentication of an image. Its purpose is to preclude the generation of an unwatermarked version of the image. That is to keep the author's identification mark clear as proof of "ownership".

For example: The paper used to print currency is heavily "watermarked". If a forger could obtain the real paper the resulting currency would still be counterfeit, even though it is on genuine paper. Thus, watermarking does not guarantee the currency is authentic.

Notes on The Role of the Random String in Increasing the Strength of the Digital Signature

These examples and explanations show how the use of one time and random elements increase the resistance of a digital signature to successful fraudulent impersonation.

Starting with a blank image and a constant signature algorithm:
Any true image could be altered to blank and the signature from a truly blank image could be added. The resulting altered image would be improperly validated as authentic with little effort. This is a weaker situation and an undesirable outcome as the same image generates the same signature.

The adaptive signature:
Here a signature is generated from the contents of the image. In the case of a blank image the same signature would be generated. An image could be manipulated to blank and the signature duplicated from a properly signed blank image. This would allow the improper validation as authentic in a manner similar to the preceding. This is still an undesirable outcome.

An adaptive signature with one time elements:
The addition of one time elements (never repeated elements such as date-time or image sequence number) allow for differing signatures even if the image itself is blank. Some convolution or manipulation of these one time elements is desirable to preclude their easy forgery. This is a stronger solution as the same image generates differing signatures.

An adaptive signature with one time and a random element:
A "random string" is a sequence of characters generated from variables including selected values from a previous image. The algorithm to create the random string is a trade secret and may differ from device to device even among the same production run of otherwise identical devices. The algorithm used may also vary from use to use of the same device. Two blank images captured a second apart with the same device can generate two widely different signatures. Two blank images captured at the exact same moment by two different devices can generate two widely different signatures. This is a stronger solution.

An adaptive signature with one time elements and one time random elements:
The user has control over how often a new random string is created. If the random string were created anew after each image was captured, then pattern recognition of the resulting signature from the image is not possible as random elements, by definition, are not patterned. Unless the signature generation protocol and the random string generation algorithm were known or reverse engineered, the ability to sign a properly constituted Signa2 image resides solely inside the Signa2 devices. By varying the random string

generation protocol between devices, varying between protocols between use to use of the same device, and regenerating the random string frequently, analysis of the results to determine the process (a form of reverse engineering) is an almost fruitless exercise.

Notes on Probability that an Authenticated File is in Fact Authentic

The MD5 signature protocol (as an example of signature protocols in general) is 160 bits long. The stated probability that the authenticated file is in fact authentic is two to the length of MD5 results in bits to one. That is: if the MD5(BLOCK) is 160 bits then the probability that an authenticated file is in fact authentic is 2^{160} : 1 or

$$2^{160}=1.46150163733090292e+48 \text{ to } 1$$

In easier to understand terms, if the odds on winning the Big Game Lottery or the Multi State PowerBall Lottery are 80 million to 1 per occurrence then these odds are the same of winning the lottery six times in a row. That is you'd have to win the lottery six times in a row to match the probability that a properly validated image using the 160 bit MD5 signature protocol was, in fact, invalid.

The odds can be further improved by processing algorithms to eliminate the possibility of false positives during authentication. Other techniques, such as encryption, can be layered over this to improve the security, but somewhere there is a balancing point between processing time and security.

Proof a = event that authentication is correct
Pa = probability that authentication is correct = 2^{160}
w = event winning the Big Game Lottery or PowerBall Lottery
Pw = probability of winning = 1 / 80,000,000

If Pw=Pa
Then $(8 * 10^7)^x = 2^{160}$
$x = \ln\ 2^{160}\ / \ln 8 \cdot 10^7$
$x = 160 \ln 2 / (\ln 8 + 7\ln 10)$
$x = 160 \ln 2 / (\ln 8 + (7\ln 5/\ln 2)\ )$
$x = 160 / 26.25 = 6.095238$

Again, you'd have to win the lottery six times in a row to match the probability that a **properly validated image** using the 160 bit MD5 signature protocol was invalid.

This is \\ P3500 \ ... \vg\Signa2-Brief-V2a