Non-Deforming Digital Watermarks

Gideon Samid
D&G Sciences – Virginia Technology Corporation
P.O.Box 1022 McLean VA 22101-1022
www.dgsciences.com
Gideon@dgsciences.com
703.385.4144

TaKE cryptography offers subliminal marking of a digital stream so that any tampering, induces an unacceptable distortion of the primary information. Encrypted audio and video streams are decrypted by one key to the original content (e.g. music), and through another key to the digital watermark (e.g. name of legitimate user). Unlike the prevailing methods which are based on distorting the protected contents, or locking it through a digital signature, TaKE -- Tailored Key Encryption -- preserves the integrity of the original stream, and its digital watermarks are inconspicious. Daniel (tm) is a particular TaKE cryptography which also offers an instant and flexible trade off between security level and speed and convenience level. The described method is fast and proper for both high capacity stream, and secrecy sensitive streams..

Contents:

The Need

In the pre-digital era information was carried on media which was amenable to demarcation and differentiation. Authors, artists, and owners marked their intellectual expressions with signatures, time stamps, tracking information, and general annotation. This added information, is commonly referred to as water marks. A term drawn from the technology to mark writing pads so that the contents of a letter would be clearly associated with the user of the marked paper. Watermarks are associated with two main features:

- 1. inconspicuousness
- 2. non-separability

In a digital format it is not trivial to achieve either attribute, and less so for the two together.

While it is possible to append a small header or trailer to a binary string, it is readily separable. Also, it is possible to sign a document in a separation-resistant manner, but then it is hardly inconspicuous.

Among the various situations where such need arises, one finds the case where a digital stream is to be interpreted through a common interpreter, and then processed for human consumption. Such is the case of digital audio and digital video. The two formats are now subject of a bitter copyright battle.

Current Solutions

Digital watermarks are applied in two basic modes:

- induced deformation
- digital signature technology

The former is based on the notion that at the human consumption stage, the digital stream can suffer a certain amount of unnoticeable deformation. This provides the opportunity to induce information-bearing changes to the digital flow, and thereby effect the watermarks.

The latter is based on the notion that one could encrypt a digital stream in conjunction with watermarks data, to create a combined stream which resists separation.

The two methods have weaknesses as outlined below.

Induced Deformation

The method: A given digital stream undergoes a slight deformation in a way that differentiates it from another copy of the same stream which may undergo a similar but distinct digital modification. When the distinctly modified streams are 'played out' for human consumption they look, or sound the same. The deformity is of such minute measure that it is not noticeable by the end user. Alas, a digital reader will be able to spot and read the digital changes and act upon such detection. The response action might be a refusal to 'play', a note to the owner, or any other action as dictated by policy.

Watermarks may be used in non-adversarial circumstances and up to very adversarial circumstances. In the latter case, one must analyze the options for an adversary to rebuff the watermarkings. We distinguish between two cases:

- 1. a valid deformation must be kept in tact.
- 2. the tracking capability must be negated.

In the first case an adversary will want to either substitute a given mark with another valid mark (to deflect a tracer), or to create a valid looking deformation to avoid rejection. The second case is easier. An adversary will need only to deform the deformity and thus erase the information therein.

In general this method will not hold against a very determined adversary. However, the prize of voiding the watermarks is usually not too high, and so all that is necessary is to make it sufficiently difficult for the adversary, so that she would drop the case.

Erasing Deformation-based Watermarks

Two basic methods are under consideration:

- 1. adding deformation.
- 2. averaging deformation.

In the first method one simply adds deformation to the digital stream and thereby erases the tracking data that was introduced through the original marks. This may increase the deformity of the final expression of the digital stream but if the original deformation was so small that it would remain unnoticeable, then double dose can not be all that harmful.

In the second method one mixes and averages out two or more deformed streams to create a mixed one which does not track to any of the participants in the mixture.

Digital Signature Technology

While the full arsenal of encryption methods may be employed in fast connecting the watermark data with the subject stream, the difficulty lies in the fact that the bona fide user would have to be given decryption tools which would yield a 'naked' subject stream. In most copyright protection cases, the threat is that a single bona fide user would then copy the unmarked digital stream and distribute it illegally. This would render the encryption protection useless.

In a way, it is the very strength of digital signature procedures that offers a weakness here. A good combination of the signature or watermark data with the subject stream is cross affecting all the bits of the signed or marked output, which creates a highly deformed output, not fit for direct 'play'.

The Proposed Solution

To employ TaKE -- Tailored Key Encryption; specifically Daniel. (For formal description see the electronic publications of the IACR -- the International Association for Cryptologic Research, at: http://eprint.iacr.org/2000. Publication: 2000/11). In essence TaKE cryptography is characterized by the attribute of multiple decryptions of the same cipherstream. Using one key, the cipherstream reads as one plainstream, and using another key – the same cipherstream is interpreted as a second

plainstream. Any changes to the cipherstream will distort the reading of *both* plainstreams. The first plainstream may be the content (audio, video) of the original stream, and the second plainstream may be some tracking data, (signatures, time stamp, legitimate user, etc.) The description below refers to a particular TaKE cryptography: Daniel, which is a trade mark, and is developed by AGS Encryptions, Ltd.

Note: TaKE cryptography, and Daniel in particular claim Shannon Security (See electronic publications of the IACR -- the International Association for Cryptologic Research, at: http://eprint.iacr.org/2000/059/). However, the application here trades security for speed and convenience. The implementer will be able to control the degree of this trade off. In the basic version described below, the security is not very high, but processing speed is very good.

The original data stream is Daniel encrypted into a somewhat longer stream, and the excess data is used to imprint the digital watermark. The cipherstream is fast decrypted into the original data stream, which may instantly (bit by bit) be translated into the analog form -- the human consumption format.

The cipherstream may also be decrypted with a watermark key to produce the watermark data.

As mentioned above, In TaKE, a given cipherstream C may be decrypted into two or more plainstreams P1, P2 using two distinct keys K1 and K2. We denote by Km the music or media key, which decrypts C into M, the clean music, or media expression. We denote Kw as the watermark key which decrypts C into W, the watermark data. Hence:

$$C = Et(M,Km) = Et(W,Kw)$$

where Et, is a TaKE type encryption.

Or:

$$M = Dt(C,Km)\ ;\ W = Dt(C,Kw)$$

where Dt is a TaKE type decryption.

Using Daniel, the original data stream M is encrypted into C. The encryption generates some excessive bits which may be modified to imprint the watermark. That imprint is not affecting the reverse decryption into the original music stream. However, it can be individualized so that each copy of the encrypted M will carry its distinct mark.

The user will be equipped with the software that would fast decrypt the cipherstream but will not generate the bit expression of M. The decrypted M bits will be instantly translated into their analog format so as to foil an attempt to grab the clean M string for illegal distribution. This is possible because of the nature of Daniel which can decrypt an infinite cipherstring bit by bit into its original plainstream.

The user will not possess the means to read the watermarks, and may not be aware of its existence. Only the owner of the system will be able to catch a floating C and read there the distinct watermark that would pinpoint the abuser, if any.

Km may be common to a large number of different music streams. It may be placed in the music (or video) player and decrypt each piece of music served upon it.

We further discuss:

- 1. Elaboration on Daniel Encryption
- 2. Cryptanalysis

Elaboration on Daniel Encryption

The following is a description of a basic version of Daniel, as it applies to the purpose at hand.

In Daniel one encrypts a formatted input stream. The decryption is done in reverse, (symmetry).

Formatting

Any input stream is first represented through a three letters (tertiary) alphabet. (X,Y,Z), say: XYZXYYXZZZY. Next the input stream is interjected with a fourth letter, W to eliminate all instances of same letter next to each other; creating a non-repeat sequence. So: XYZXYWYXZWZWZY. As a matter of convention, the letter W is also added to the start of the string: WXYZXYWYXZWZWZY The resultant non-repeat sequence is ready for encryption.

Each of the four letters, X, Y, Z, and W is denoted as "color".

Encryption

Daniel encryption happens by interpreting the formatted input (non repeat sequence), as a "travel guide" within a map marked with zones which are colored by the four colors of the input stream. According to Cayley's four color theorem, any map, however complex may be painted with only four colors. Hence, the fact that the map is painted with four colors betrays no information about its contents.

The "map" may be as small as below:

```
X X Y
Z W Y
Z Z Y
```

The input stream: W X Y Z X Y W Y X Z W Z W Z Y taken as a traveling guide will result in a traveling sequence described as:

U R D D L L U U R D L R U L L D R L R L D R R

Where U,D,L,R represent the four steps: Up, Down, Left, Right.

Decryption happens in reverse. The traveling sequence is reduced to the traveling guide.

Without knowledge of the map, which is indeed the Daniel key, (or the music key, Km, as denoted above), the encrypted sequence can not be decrypted. The mathematical security of Daniel is hinged on the fact that given the decrypted stream, as above, it is possible to chart a map that would fit that cipherstream with a large variety of plausible plainstreams.

Also note that the input stream above could have been interpreted by many other maps, for example:

```
X X X X X X Y Y Y
X X X X X X Y Y Y
X X X X X X Y Y Y
X X X W W W Y Y Y
X X X W W W Y Y Y
X X X W W W Y Y Y
Z Z Z Z Z Z Z Z Z
Z Z Z Z Z Z Z Z Z
Z Z Z Z Z Z Z Z Z
```

Note that in the above example there are nine W elements. Traversal across these elements is meaningless for decryption purposes, since it would all be reduced to a single W letter. This latitude allows for watermarkings to be placed in these nine elements. The watermarks will be interpreted according to a watermark key, Kw, of the form:

```
W W W W W W W W W
W W W W W W W W W
W W W W W W W W W
W W W X X Y W W W
W W W X W Y W W W
W W W Z Z Z W W W
W W W W W W W W W
W W W W W W W W W
W W W W W W W W W
```

The net result is that the same cipherstream will be interpreted as the same quality music by Km, while each copy will have its own watermark as interpreted by Kw.

Cryptanalysis

Cryptanalysis may TaKE the following forms:

- 1. Replacing a valid watermark with another valid watermark.
- 2. Destroying a valid watermark to avoid detection.

For either form, the hacker would try to ascertain Km -- the music key. For the first form it is necessary to also determine Kw. It is theoretically possible to hack into this protection without cryptanalyzing Km, but this is highly unlikely.

Although Daniel is a deniability featured cryptography, this implementation does not TaKE advantage of the same.

Once Km is mapped out, the hacker would be able to identify the sections in the input stream which are likely to carry the watermark, and then this portion may be modified. If so, then the resultant input stream would play at the same quality as the original.

Cryptanalyzing km

Km, the music key per se, is not very immunized against hacking. However, the implementer determines the amount of cryptanalysis effort that will be needed, and in the context of copyright protection, and similar circumstances, such control of cryptanalytic difficulty is all that is needed. This is so especially for cases where the legal copy is not very expensive.

Methods of Attack

Km is available at the play station where the encrypted stream is decoded to its human consumption. Hence it is subject to chosen plaintext attack. To examine the output the cryptanalyst will need to choose between:

- examining the analog output
- intercepting the decrypted digital stream

Once done, the cryptanalyst will be able to explore Km with carefully designed inputs. This effort is proportional to the size of Km.

Since with Daniel the size of Km may be made as large and as complex as desired (without a meaningful adverse impact on speed), it is possible to create a large enough music key (Km).

Also, the implementer may choose to replace Km as often as needed. The replacement could be a totally new Km, or a modified old Km. In the latter case, the old inputs will play as before.

Hacking Without km

Given several copies of differently watermarked input streams, it is not helpful to simply mix them, as one does in hacking into the induced-deformation method. However, a large enough number of copies would indicate where the likely watermark is written, and with some trial and error a hacker would be able to construct a copy that would void the watermarks.

A proper defense would come from (1) increasing the complexity of Km (which the implementer can do without any other changes to the software or the hardware), (2) distributing the watermarks along the input stream, and, (3) creating redundancy.

Of course, switching to another Km will force the hacker to start all over again.

Implementation Modes

Digital watermarks are useful in many situations, and each situation leads to its own specific implementation.

Here we focus on copyright protection of digital entities (music, video) which are stream-fed for human consumption. In this situation there are usually numerous legal copies, each of them individually watermarked, and one needs to monitor any attempt to crack the watermarks and distribute untraceable illegal copies.

We discuss the case where the digital stream is downloaded through the Internet, and played back either on computers or on off-computer devices.

The off-computer playback may be executed with a fixed music key (Km), if so desired. This might serve for lower quality music, or for old pieces that are too "cold" for hacking activity anyway. Alternatively, Km can be packed together with the input stream so that the combination will play anywhere.

There are numerous marketing advantages and options based on the ability to replace or modify Km. The replacement might be in response to hacking activity, or as a time-based usage agreement. In principle, the playing computer might "ping" the Internet source for a copy of Km, each time it tries to play a piece. This would provide invaluable marketing data.

The nature of Daniel is that keys can be 'amplified'. That is, a Km can be replaced with a more involved, more complex Km which will still play the old pieces, though it would be necessary for the new pieces to be properly interpreted. The implementer will be able to respond to the actual hacking activity against its products. If it rises, then Km becomes more complex and is changed more often.

With Daniel one achieves all the necessary changes just by replacing the key, without changing any software or hardware.

Additional Reading:

The Proposed encryption scheme is featured in Daniel, Leonardo and related products distributed by D&G Sciences – Virginia Technology Corporation, 6867 Elm St. Suite 200, P.O.Box 1022, McLean, Virginia 22101-1022. 703.385.4144, www.dgsciences.com