(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 December 2000 (07.12.2000)

PCT

(10) International Publication Number
WO 00/74371 A1

(51) International Patent Classification⁷: H04N 1/32

(21) International Application Number: PCT/EP00/04053

(22) International Filing Date: 5 May 2000 (05.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
99/07139 1 June 1999 (01.06.1999) FR

(71) Applicant *(for all designated States except US)*: THOMSON MULTIMEDIA [FR/FR]; 46, quai Alphonse Le Gallo, F-92100 Boulogne-Billancourt (FR).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: FURON, Teddy [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). DUHAMEL, Pierre [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

(74) Agent: RUELLAN-LEMONNIER, Brigitte; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

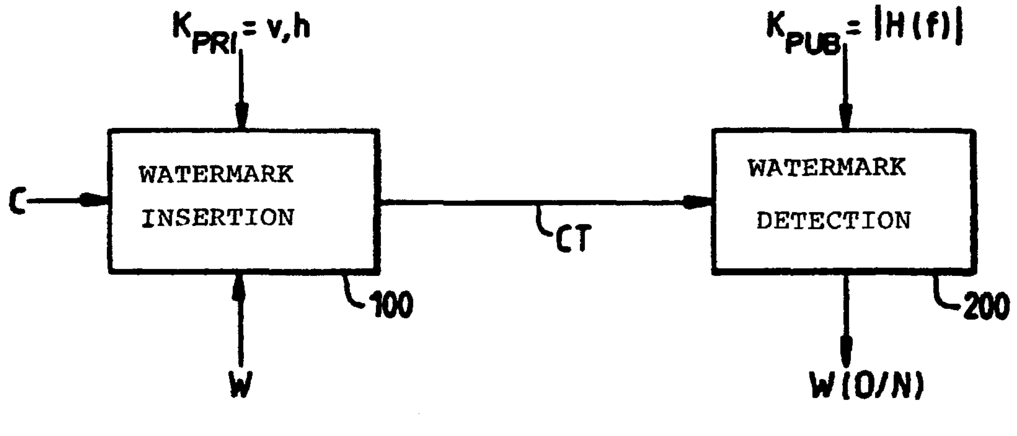
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DIGITAL DATA WATERMARKING SYSTEM USING NOVEL WATERMARK INSERTION AND DETECTION METHODS



(57) Abstract: The watermarking system uses a first series of parameters (v, h), the private key (K_{PRI}), for the insertion of the watermark, and a second series of parameters (|H(f)|), the public key (K_{PUB}), for the detection of the watermark, so that knowledge of the public key does not make it possible to know the private key and does not make it possible to delete or modify the watermark. The insertion of the watermark is performed by adding a pseudo random noise sequence (v), filtered by a filter with impulse response (h), to the data to be watermarked. The detection of the watermark is performed by searching through the data received for whether they contain noise which has been filtered by a filter with predefined spectral response (H(f)). Application to copy protection.

Digital data watermarking system using novel watermark insertion and detection methods

The present invention relates to the field of watermarking of digital data. It relates more particularly to a system for watermarking data using novel watermark insertion and detection methods as well as to devices for implementing these methods.

Recent methods for protecting against the illicit copying of digital data use the principle of data watermarking which consists in inserting a marking item, commonly referred to as a "watermark", into a multimedia content (still image, video, sound, etc.) in an imperceptible manner. The watermark can for example be a signal indicating that the content may not be copied or any other item allowing the supplier of the multimedia content to detect illegal copies.

In order to play its role perfectly, the watermark must be robust to transformations of the watermarked content, whether these transformations be made intentionally by a pirate who wishes to erase the watermark, or whether they result from distortions which occurred during the transmission of the signal containing the watermarked data.

Various data watermarking techniques are known from the prior art. Reference may in particular be made to the documents EP-A-0 828 372, EP-A-0 840 513, WO-A-98/03014 or WO-A-98/54897 which describe methods for inserting watermarks into data to be protected and methods for detecting the presence of such watermarks in the data.

A scheme which is generally used to describe the principle of data watermarking is that of Figure 1. A first part 1 relates to the insertion of a hidden item W (the watermark) into a content to be protected C. This results in a watermarked content CT. Part 2 relates to the detection of the presence of the item W in the content received CT. An additional datum K is also necessary in the process for inserting and detecting the watermark. This datum K which must be shared in a secret manner by the device for inserting and detecting the watermark is referred to as the key by analogy with so-called symmetric or private-key cryptography systems.

For example, a known watermarking technique consists in adding a pseudo random noise sequence to data which are to be watermarked. The detection process is carried out, in this case, by performing a correlation calculation: the data received are declared watermarked if the correlation with the reference pseudo noise sequence (used for the insertion of the watermark) is greater than a given threshold. In this example, the reference pseudo noise sequence constitutes the key K of the data watermarking scheme of Figure 1.

The problem with this scheme is that each entity capable of detecting the watermark must share the same key K as the entity which inserted the watermark. In this case, the entity capable of detecting the watermark can furthermore delete it or modify it, thereby doing away with all the benefit of the initial watermarking of the data. Consequently, a supplier of content protected by watermarking should not communicate his key K, which served for the insertion of the watermark, other than in a secret manner to trusted entities. This considerably limits the possibilities of using data watermarking in numerous fields.

In particular, in the field of consumer electronic appliances, it is well known that it is almost impossible, at any event at reasonable cost, to store secret parameters in an appliance or in software contained in such an appliance. Smart cards, which are regarded as the only pieces of equipment allowing the secure storage of a secret parameter, are not themselves powerful enough to perform the calculations connected with a watermark detection process.

In the example described above where the watermarking is carried out by adding a pseudo random noise sequence to the data which are to be watermarked, even if the reference pseudo noise sequence is stored secretly in the watermark detection device, it has been demonstrated that a pirate can theoretically discover the reference sequence and thus delete the watermark from the data by observing the output from the detector as a function of a large number of different input signals.

The invention aims to solve the aforesaid problems.

To this end, the invention relates to a method for inserting a watermark into data representing a content to be protected. According to the invention, the method comprises the steps consisting in:

a) supplying a pseudo random noise sequence to the input of a filter with predefined impulse response; and

b) adding the filtered pseudo noise sequence to the data.

According to a preferred aspect of the invention, the method furthermore comprises the steps consisting in:

c) performing a pseudo random interleaving of the data before step b); and

d) performing an inverse interleaving after step b) so as to obtain the watermarked data.

The invention also relates to a method for detecting a watermark in data representing a content received, characterized in that it comprises the steps consisting in:

i) performing a spectral analysis of the data; and

ii) deducing therefrom whether the data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response.

According to another preferred aspect of the invention, a pseudo random interleaving of the data received, which is identical to the interleaving performed in step c) above, is performed before step i).

The invention also relates to a system for watermarking data using a watermark insertion method and a watermark detection method as those above. According to the invention, a first series of parameters, the private key, is used for the insertion of the watermark and a second series of parameters, the public key, is used for the detection of the watermark, so that:

- knowledge of the public key does not make it possible to know the private key; and

- knowledge of the method of detection and of the public key does not make it possible to delete or modify the watermark.

The invention also relates to a device for inserting a watermark into data representing a content to be protected. According to the invention, the device comprises:

- means for generating a pseudo random noise sequence;

- filtering means having a predefined impulse response and which are adapted for receiving the pseudo noise sequence and for supplying a filtered pseudo noise sequence; and

- means for adding the filtered pseudo noise sequence to the data.

According to a preferred embodiment of the invention, the device furthermore comprises:

- first means of pseudo random interleaving of the data representative of the content to be protected so as to supply interleaved data, the interleaved data being supplied to the addition means so as to be added to the filtered pseudo noise sequence; and

- means of inverse interleaving of the first interleaving means, linked to the output of the said addition means so as to supply the watermarked data.

According to a particular embodiment of the invention, the device comprises:

- means for transforming the content to be protected into data representative of the content;

- means for generating a modulation sequence indicative of the maximum amount of noise which can be added to the data;

- first means of pseudo random interleaving of the data representative of the content to be protected so as to supply interleaved data;

- second means of pseudo random interleaving, which are identical to the first adapted for receiving the modulation sequence so as to supply an interleaved modulation sequence;

- multiplication means adapted for receiving, on the one hand the interleaved modulation sequence, and on the other hand the filtered pseudo noise sequence, so as to supply the watermark;

- means of addition of the interleaved data and of the watermark, the output of the addition means being linked to:

- means of inverse interleaving of the first and second interleaving means so as to supply the watermarked data; and

- means of inverse transformation of the watermarked data into a marked content.

The invention also relates to a device for detecting a watermark in data representing a content received. According to the invention, the device comprises:

- means for estimating the power spectral density of the data; and

- means of likelihood testing of hypotheses so as to estimate whether the data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response.

According to a particular embodiment, the device furthermore comprises:

- means of pseudo random interleaving of the data representing the content received, which are adapted for performing the same interleaving as the first interleaving means of the insertion device, the interleaved data being supplied to the means for estimating the power spectral density.

According to another particular embodiment, the device furthermore comprises:

- means for transforming the content received into data representative of the content, the transforming means being adapted for performing the same transformation as the transforming means of the insertion device.

Other characteristics and advantages of the invention will become apparent on reading the following description of a particular embodiment, which is non-limiting, of the invention given with reference to the appended figures, among which:

- Figure 1, described previously, illustrates a known scheme for watermarking digital data;
- Figure 2 schematically represents a watermark insertion device according to the invention;
- Figure 3 schematically represents a watermark detection device according to the invention;
- Figure 4 illustrates a novel scheme for watermarking digital data according to the invention.

Represented schematically in Figure 2 is a device according to the invention for inserting a watermark into a signal representative of a content to be protected. This signal can in particular be a digital video or audio signal or else a signal representing a still image such as a photograph or a computer-calculated synthetic image, or more generally, any signal representing a multimedia content.

Firstly, the content to be protected is transformed by a transformation module 10 into a sequence of digital data $\mathbf{x} = \{x_n\}$, n lying between 1 and N. For example, if the content to be protected is an image comprising N pixels, the coefficients x_n can correspond to the luminance of each pixel of the image. These may also be coefficients of a Discrete Fourier Transform of the signal representing the content to be protected, or else coefficients of a Fourier-Mellin Transform or coefficients of a wavelet decomposition when the content to be protected is a still image.

The data sequence **x** representing the content to be protected is transmitted on the one hand to a module HPM 12 which outputs a modulation sequence $\mathbf{m} = \{m_n\}$, $\forall n \in [1..N]$. The module HPM calculates this modulation sequence as a function of algorithms based on human perception models, such as Sarnoff's model of the eye. This sequence $\mathbf{m} = \{m_n\}$ represents the maximum amount of noise which can be added to each coefficient x_n without perceptible loss of quality.

According to one aspect of the invention, the data sequence **x** is transmitted moreover to an interleaver 20, which performs a random permutation p of the coefficients x_n so as to supply a sequence of interleaved coefficients $\tilde{\mathbf{x}} = \{x_{p(n)}\}$. The purpose of this interleaving of the data sequence **x** will be explained subsequently.

The modulation sequence **m** is also transmitted to an interleaver 14 which performs the same permutation p of the coefficients m_n as that performed by the interleaver 20 so as to output an interleaved modulation sequence $\tilde{\mathbf{m}} = \{m_{p(n)}\}$.

In order to constitute the watermark which will be inserted into the data sequence **x** representing the content to be protected, a pseudo random noise generator (not represented) firstly supplies a pseudo noise sequence $\mathbf{v} = \{v_n\}$, $\forall n \in [1..N]$, with Gaussian distribution. This pseudo noise sequence **v** is transmitted to the input of a filter 16, of Linear Time Invariant (LTI) type, whose impulse response is:

$\mathbf{h} = \{h_n\}$, $\forall n \in [1..L]$ where L is an integer corresponding to the length of the filter;

and whose spectral response is H(f), H(f) being the Fourier Transform of **h**.

At the output of the filter 16 one obtains a filtered pseudo noise sequence $\mathbf{w} = \{w_n\}$, $\forall n \in [1..N]$ satisfying the following equation (1):

$$w_n = \sum_{k=1}^{L} v_{n-k} \cdot h_k = h_n \otimes v_n \qquad \forall n \in [1..N] \qquad (1)$$

in which ⊗ represents the convolution product.

From this may be deduced, from the interference theorem, the following two equations (2) and (3):

$$\varphi_{ww}(\tau) = (\mathbf{h} \otimes \mathbf{h}) \otimes \varphi_{vv}(\tau) \qquad (2)$$

in which $\varphi_{ww}(\tau)$ and $\varphi_{vv}(\tau)$ respectively represent the auto-correlation functions of **w** and of **v**; and

$$\Phi_{ww}(f) = |H(f)|^2 \cdot \Phi_{vv}(f) \qquad (3)$$

in which $\Phi_{ww}(f)$ and $\Phi_{vv}(f)$ respectively represent the power spectral densities of $\varphi_{ww}(\tau)$ and $\varphi_{vv}(\tau)$, that is to say their Fourier Transforms.

Since **v** is a pseudo random noise sequence with Gaussian distribution, its spectrum, that is to say the function $\Phi_{vv}(f)$, has a substantially flat shape. On the other hand, once this sequence **v** is filtered by the filter 16, the resulting sequence **w** exhibits a spectrum $\Phi_{ww}(f)$ which is no longer flat on account of the term $|H(f)|^2$. It is also important to note, so as to comprehend the rest of the invention, that knowledge of $|H(f)|^2$ (and by the same token, knowledge of the modulus of H(f):|H(f)|) does not make it possible to retrieve H(f) (and hence **h**) since there is an uncertainty with regard to the phase of H(f).

Returning to Figure 2, the filtered pseudo noise sequence **w** is multiplied (multiplier 18) by the interleaved modulation sequence $\tilde{\mathbf{m}}$ and the resulting sequence, which constitutes the watermark, is added (adder 22) to the sequence of interleaved data $\tilde{\mathbf{x}}$.

The output sequence from the adder 22 is denoted $\tilde{\mathbf{y}}$ = $\{y_{p(n)}\}$ and satisfies the following equations (4) and (5):

$$y_{p(n)} = x_{p(n)} + m_{p(n)} \cdot \left(h_n \otimes v_n\right) \qquad (4)$$

$$\tilde{\mathbf{y}} = \tilde{\mathbf{x}} + \tilde{\mathbf{m}} \cdot \left(\mathbf{h} \otimes \mathbf{v}\right) \qquad (5)$$

The power spectral density of the sequence of watermarked interleaved data $\tilde{\mathbf{y}}$ is given by the following equations (6) and (7):

$$\Phi_{\tilde{y}\tilde{y}}(f) = \Phi_{\tilde{x}\tilde{x}}(f) + \Phi_{\tilde{m}\tilde{m}}(f) \cdot \Phi_{h \otimes v}(f) \qquad (6)$$

$$\Phi_{\tilde{y}\tilde{y}}(f) = \left(\mu_x^2 \cdot \delta(f) + \sigma_x^2\right) + \left(\sigma_m^2 \cdot \sigma_v^2 \cdot \sum_u h_u^2\right) + \mu_m^2 \cdot \sigma_v^2 \cdot \left|H(f)\right|^2 \qquad (7)$$

In equation (7), μ_j and σ_j respectively represent the mean and the standard deviation of the sequence $\mathbf{j}$ = $\{j_n\}$ with j ∈ {x, m, v}, δ(f) corresponds to the Dirac pulse and the expression $\left(\sigma_m^2 \cdot \sigma_v^2 \cdot \sum_u h_u^2\right)$ is equal to a constant.

The sequence of watermarked interleaved data $\tilde{\mathbf{y}}$ is then transmitted to an inverse interleaver 24 which performs the operation inverse to the permutation p performed by the interleavers 20 and 14 so as to supply a sequence of watermarked data $\mathbf{y}$ = $\{y_n\}$ whose coefficients are in the same order as the initial order of the data $\mathbf{x}$ = $\{x_n\}$.

A transformation inverse to that performed by the transformation module 10 is then performed by the module 26 so as to obtain the marked content (or watermarked content) which is thus protected against illicit copying without the watermark being perceptible within the content.

We shall now describe, in conjunction with Figure 3, a device for detecting a watermark in a received content when this watermark has been inserted into a content to be protected by a device such as that of Figure 2.

The principle of the detection is based on the spectral analysis of the signal received.

The signal received is representative of the received content for which one will seek to determine whether or not it is watermarked. This content is of the same type as the content to be protected described previously. In the example which follows, it will be assumed that the content received is an image containing N pixels.

The content received is firstly transmitted to a transformation module 30 which performs the same transformation operation as the module 10 of the watermark insertion device of Figure 2 so as to supply a data sequence $\mathbf{r} = \{r_n\}$, $\forall n \in [1..N]$ representing the content received. In our example, it is assumed that the luminances r_n of the pixels of the image received are obtained as output from the transformation module 30.

If the content received were to correspond exactly to the watermarked content emanating from the device of Figure 2, that is to say if no transformation or distortion of the signal had taken place during transmission between the watermark insertion device and the detection device, then one would have:

$$\mathbf{r} = \{r_n\} = \mathbf{y} = \{y_n\}$$

In practice, this is not always the case since the signal sometimes undergoes transformations during its transmission.

Since the watermark has been inserted, in the device of Figure 2, into a sequence of interleaved data $\tilde{\mathbf{x}}$, the data sequence $\mathbf{r}$ will, in order to detect the possible presence of a watermark in the content received, be transmitted to an interleaver 32 performing the same permutation p of the coefficients r_n as that performed by the interleavers 20 and 14 of Figure 2.

A sequence of interleaved data $\tilde{\mathbf{r}} = \{r_{p(n)}\}$ is obtained as output from the interleaver 32.

It was seen previously that when the watermark inserted is a pseudo noise sequence filtered by a filter with impulse response $\mathbf{h}$ and with spectral response H(f), the power spectral density of the (interleaved) data obtained $\tilde{\mathbf{y}}$ is expressed by relations (6) and (7).

The purpose of the interleaving of the data sequence **x** and of the modulation sequence **m** will now be apparent. Indeed, if the data sequence **x** represents the pixels of an image, its spectral density has a very structured shape with very large amplitude differences. The role of the interleaving of the data is to sever the statistical coherence of this sequence so that the spectral density of the sequence of interleaved data $\tilde{\mathbf{x}}$ has a substantially flat shape, such as that of a pseudo noise sequence with Gaussian distribution.

Thus, if a watermark consisting of a pseudo noise sequence filtered by a filter with spectral response H(f) is added to this interleaved sequence, a data sequence is obtained whose power spectral density can be expressed by relation (7) in which the significant term $|H(f)|^2$ can be detected.

The principle of the detection will therefore be based on the spectral analysis of the sequence $\tilde{\mathbf{r}}$ and on a Maximum Likelihood Ratio Hypothesis test (MLR Hypothesis test), the hypothesis tested being the following: if the sequence of interleaved data $\tilde{\mathbf{r}}$ contains noise, is it noise which has been filtered by a filter whose spectral response has a modulus similar to $|H(f)|$? If the response is yes, one will deduce from this that the noise present in the sequence $\tilde{\mathbf{r}}$ is a watermark and, in the contrary case, one will conclude from this that the content received was not watermarked.

In practice, this analysis is based on calculations relating to spectral analysis and the likelihood testing of hypotheses which are described in detail in the work by K. Dzhaparidze, *"Parameter Estimation and Hypothesis Testing in Spectral Analysis of Stationary Time Series"*, Springer Series in Statistics, Springer-Verlag, 1986, to which reference may be made for further details.

Returning to Figure 3, the sequence of received interleaved data $\tilde{\mathbf{r}}$ is transmitted to a module 34 performing a Periodogram calculus. This calculus is aimed at estimating the power spectral density of the sequence $\tilde{\mathbf{r}}$. A quantity $I_N(f)$ given by the following relation (8)

$$I_N(f)=\frac{1}{N}\left|\sum_{k=1}^{N}\tilde{r}_k\cdot\exp(2\pi jfk)\right|^2 \qquad (8)$$

is obtained at output.

This quantity is then transmitted to a module 36 performing a MLR Hypothesis test so as to determine whether the content received is watermarked (output response "Y") or not (output response "N").

The module 36 tests the likelihood of two hypotheses:

- according to the first hypothesis G_0, the content received is not watermarked, hence the spectral density of the sequence $\tilde{\mathbf{r}}$ is substantially flat and can be estimated via the following relation (9):

$$g_0(f)=\sigma_r^2+\mu_r^2\cdot\delta(f) \qquad (9)$$

- according to the second hypothesis G_1, the content received is watermarked and the spectral density of the sequence $\tilde{\mathbf{r}}$ can be estimated via the following relation (10):

$$g_1(f)=\mu_m^2\cdot\sigma_v^2\cdot|H(f)|^2+C \qquad (10)$$

in which C is a constant and σ_v is equal to 1 (one preferably chooses the pseudo noise sequence **v** at the level of the insertion device so that σ_v is equal to 1, but one may equally choose other values). Furthermore, μ_m is normed at the level of the insertion device and equals for example 3.

To estimate the likelihood of the hypotheses G_0 and G_1, the module 36 calculates two numbers $U_{N,0}(\tilde{\mathbf{r}})$ and

$U_{N,1}(\tilde{\mathbf{r}})$ representing the likelihoods of the hypotheses G_0 and G_1 according to the following relation (11):

$$U_{N,i}(\tilde{\mathbf{r}}) = -\int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\log g_i(f) + \frac{I_N(f)}{g_i(f)} \right) df \quad \text{with } i \in \{0,\ 1\} \quad \mathbf{(11)}$$

By then comparing these two numbers, the module 36 deduces from this:

- if $U_{N,1}(\tilde{\mathbf{r}}) > U_{N,0}(\tilde{\mathbf{r}})$, then the response of the detector is "Y" signifying that the content received is watermarked; and

- if $U_{N,1}(\tilde{\mathbf{r}}) < U_{N,0}(\tilde{\mathbf{r}})$, then the response of the detector is "N" signifying that the content received is not watermarked.

It is also possible, in a preferential manner, to calculate the difference $(U_{N,1}(\tilde{\mathbf{r}}) - U_{N,0}(\tilde{\mathbf{r}}))$ and to perform the above comparisons only if this difference is greater than a predetermined threshold, this being so as to guarantee better exactness of detection.

The watermark insertion and detection methods just described with reference to Figures 2 and 3 make it possible to produce a novel watermarking system which is illustrated by Figure 4. In this novel system and according to a preferred aspect of the invention, a parameter which is referred to as the "private key" K_{PRI} is used for the insertion (100) of a watermark W into a content C, whereas another parameter which is referred to as the "public key" K_{PUB} is used for the detection (200) of a watermark in a content received CT. The terms "private key" and "public key" are used by analogy with public key crytographic systems. It will be noted that here the watermark W is binary, that is to say that, either the content C is watermarked, or it is not, but W does not contain any item of its own.

In the embodiment described above, the private key K_{PRI} is formed by the pseudo random noise sequence $\mathbf{v}$ as well as by the impulse response $\mathbf{h}$ of the filter 16 (Fig. 2). The sequences $\mathbf{v} = \{v_n\}$ and $\mathbf{h} = \{h_n\}$ are in effect indispensable to the calculation of the sequence

$\mathbf{w} = \{w_n\}$ which is itself, after having been multiplied by the interleaved modulation sequence $\tilde{\mathbf{m}}$, inserted into the data representing the content to be protected.

The public key used to detect the watermark in the content received is for its part formed from the modulus of the spectral response of the filter 16 $|H(f)|$. Indeed, in the spectral analysis calculations performed (modules 34 and 36 of Figure 3) to detect the presence of a watermark in a content received CT, only the knowledge of $|H(f)|$ is necessary. In particular, it is not necessary to know **v** and **h** (the private key) to perform the detection of the watermark. In actual fact, as was seen earlier in the description, the knowledge of $|H(f)|$ does not suffice to know $H(f)$ and hence **h**.

A system is therefore obtained in which knowledge of the public key does not make it possible to deduce the private key from this. Also, not knowing the private key, it is impossible for the device performing the detection of the watermark to delete it or to modify it. The detection can therefore be performed in a non-secure environment with no risk of the watermark being erased.

CLAIMS

1. Method for inserting a watermark into data (**x**) representing a content to be protected, characterized in that it comprises the steps consisting in:

a) supplying a pseudo random noise sequence (**v**) to the input of a filter with predefined impulse response (**h**); and

b) adding said filtered pseudo noise sequence (**w**) to said data.

2. Method according to Claim 1, characterized in that it furthermore comprises the steps consisting in:

c) performing a pseudo random interleaving (p) of the data (**x**) before step b); and

d) performing an inverse interleaving after step b) so as to obtain the watermarked data.

3. Method for detecting a watermark in data (**r**) representing a content received, characterized in that it comprises the steps consisting in:

i) performing a spectral analysis of said data; and

ii) deducing therefrom whether said data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response (H(f)).

4. Method according to Claim 3 for detecting a watermark in data (**r**) representing a content received, the watermark being adapted to be inserted in accordance with the method according to Claim 2, characterized in that it furthermore comprises a step consisting in:

iii) performing, before step i), a pseudo random interleaving (p) of the data (**r**) received, which is identical to the interleaving performed in step c).

5. Watermarking System using a watermark insertion method according to one of Claims 1 or 2 and a watermark detection method according to one of Claims 3 or 4, characterized in that a first series of

parameters (**v**, **h**), the private key (K_{PRI}), is used for the insertion of the watermark and a second series of parameters ($|H(f)|$), the public key (K_{PUB}), is used for the detection of the watermark, so that:

- knowledge of the public key does not make it possible to know the private key; and
- knowledge of the watermark detection method and of the public key does not make it possible to delete or modify the watermark.

6. Device for inserting a watermark into data (**x**) representing a content to be protected, characterized in that it comprises:

- means for generating a pseudo random noise sequence (**v**);
- filtering means (16) having a predefined impulse response (**h**) and which are adapted for receiving said pseudo noise sequence (**v**) and for supplying a filtered pseudo noise sequence (**w**); and
- means (22) for adding said filtered pseudo noise sequence (**w**) to said data (**x**).

7. Device according to Claim 6, characterized in that it furthermore comprises:

- first means (20) of pseudo random interleaving of the data (**x**) representative of the content to be protected so as to supply interleaved data ($\tilde{\mathbf{x}}$), said interleaved data being supplied to the addition means (22) so as to be added to the filtered pseudo noise sequence (**w**); and
- means (24) of inverse interleaving of said first (20) interleaving means, linked to the output of said addition means (22) so as to supply the watermarked data.

8. Device according to Claim 6, comprising:

- means (10) for transforming the content to be protected into data (**x**) representative of said content;
- means (12) for generating a modulation sequence (**m**) indicative of the maximum amount of noise which can be added to said data;

characterized in that it furthermore comprises:

- first means (20) of pseudo random interleaving of said data ($\mathbf{x}$) representative of the content to be protected so as to supply interleaved data ($\tilde{\mathbf{x}}$);

- second means (14) of pseudo random interleaving, which are identical to the first (20) adapted for receiving said modulation sequence ($\mathbf{m}$) so as to supply an interleaved modulation sequence ($\tilde{\mathbf{m}}$);

- multiplication means (18) adapted for receiving, on the one hand the interleaved modulation sequence ($\tilde{\mathbf{m}}$), and on the other hand the filtered pseudo noise sequence ($\mathbf{w}$), so as to supply the watermark;

- means (22) of addition of the interleaved data ($\tilde{\mathbf{x}}$) and of the watermark, the output of said addition means being linked to:

- means (24) of inverse interleaving of said first (20) and second (14) interleaving means so as to supply the watermarked data ($\mathbf{y}$); and

- means (26) of inverse transformation of the watermarked data into a marked content.

9. Device for detecting a watermark in data ($\mathbf{r}$) representing a content received, characterized in that it comprises:

- means (34) for estimating the power spectral density of said data; and

- means (36) of likelihood testing of hypotheses so as to estimate whether said data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response (H(f)).

10. Device according to Claim 9, adapted for detecting a watermark inserted by an insertion device according to one of Claims 7 or 8, characterized in that it comprises:

- means (32) of pseudo random interleaving of the data ($\mathbf{r}$) representing the content received, which are adapted for performing the same interleaving (p) as said first interleaving means (20) of the insertion device, said interleaved data ($\tilde{\mathbf{r}}$) being supplied to said means (34) for estimating the power spectral density.

11. Device according to Claim 10, adapted for detecting a watermark inserted by an insertion device according to Claim 8, characterized in that it furthermore comprises:

- means (30) for transforming the content received into data (**r**) representative of said content, said transforming means being adapted for performing the same transformation as the transforming means (10) of the insertion device.

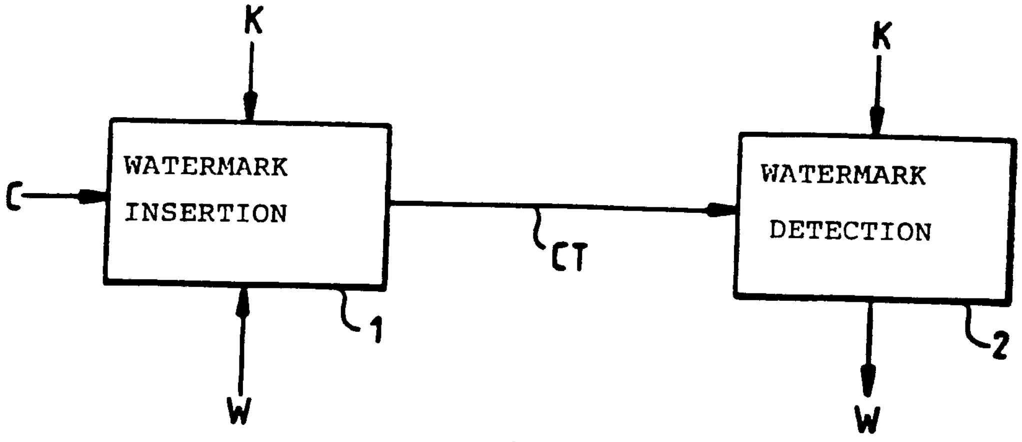

K
K
C
WATERMARK INSERTION
CT
WATERMARK DETECTION
1
2
W
W

FIG.1

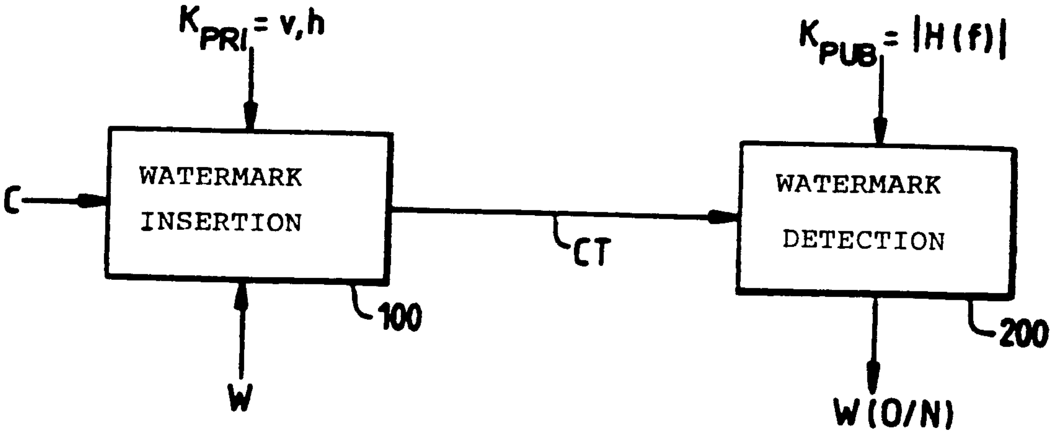

$K_{PRI} = v,h$
$K_{PUB} = |H(f)|$
C
WATERMARK INSERTION
CT
WATERMARK DETECTION
100
200
W
W(O/N)

FIG.4

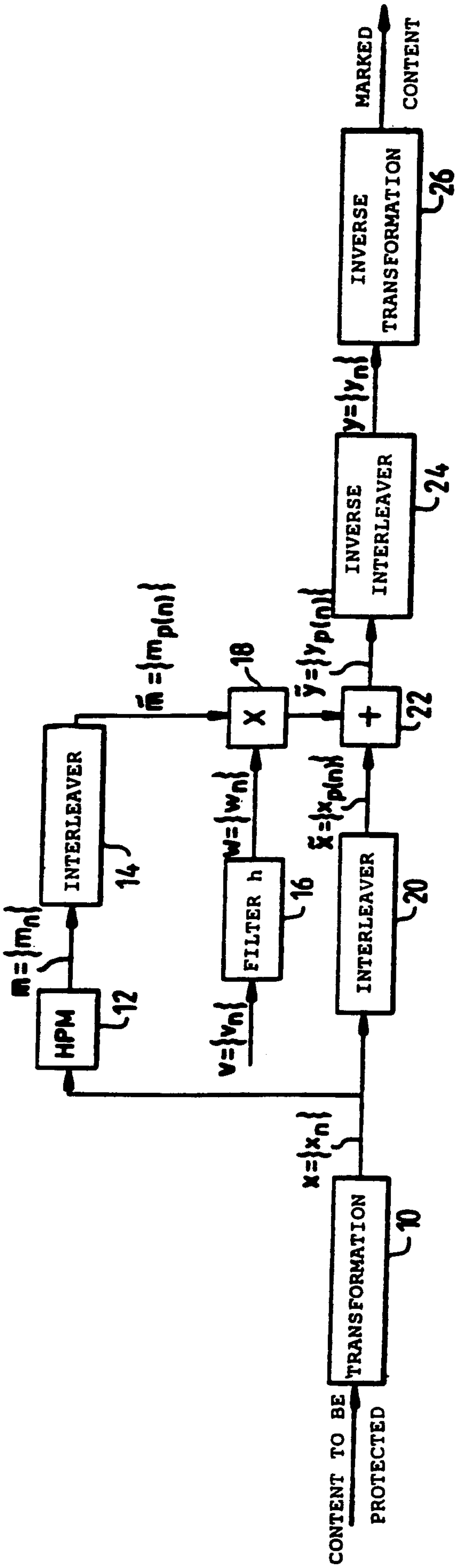

CONTENT TO BE PROTECTED
TRANSFORMATION
10
x={xn}
HPM
12
m={mn}
INTERLEAVER
14
m̃={mp(n)}
v={vn}
FILTER h
16
w={wn}
X
18
INTERLEAVER
20
x̃={xp(n)}
+
22
ỹ={yp(n)}
INVERSE INTERLEAVER
24
y={yn}
INVERSE TRANSFORMATION
26
MARKED CONTENT

FIG. 2

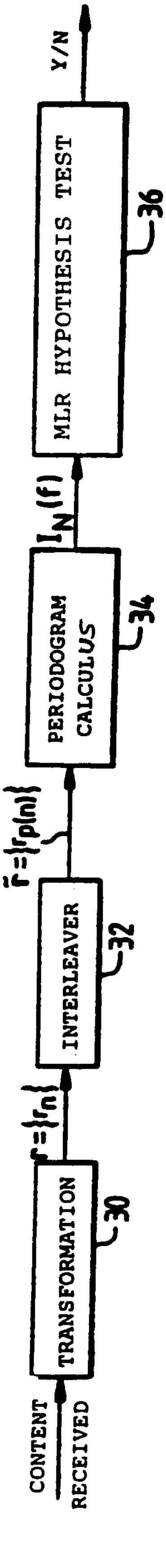

CONTENT RECEIVED
TRANSFORMATION
30
r={rn}
INTERLEAVER
32
r̃={rp(n)}
PERIODOGRAM CALCULUS
34
IN(f)
MLR HYPOTHESIS TEST
36
Y/N

FIG. 3

INTERNATIONAL SEARCH REPORT

Intern ıal Application No
PCT/EP 00/04053

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 766 468 A (NIPPON ELECTRIC CO) 2 April 1997 (1997-04-02) abstract column 6, line 40 -column 9, line 6 ---	1-4,6,7
A	EP 0 840 513 A (NIPPON ELECTRIC CO) 6 May 1998 (1998-05-06) abstract column 3, line 40 -column 4, line 16 column 4, line 49 -column 7, line 22 ---	1-4,6,7
A	US 5 499 294 A (FRIEDMAN GARY L) 12 March 1996 (1996-03-12) abstract --- -/--	5

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 31 July 2000	Date of mailing of the international search report 04/08/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Hubeau, R

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/EP 00/04053

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 748 783 A (RHOADS GEOFFREY B) 5 May 1998 (1998-05-05) abstract column 2, line 51 -column 4, line 8 -----	8,10

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr nal Application No

PCT/EP 00/04053

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0766468 A	02-04-1997	AU 701639 B	04-02-1999
		AU 6584096 A	10-04-1997
		CA 2184949 A	29-03-1997
		JP 9191394 A	22-07-1997
		US 5930369 A	27-07-1999
EP 0840513 A	06-05-1998	US 5915027 A	22-06-1999
		AU 4434097 A	07-05-1998
		CA 2219205 A	05-05-1998
		JP 10145757 A	29-05-1998
		SG 63773 A	30-03-1999
US 5499294 A	12-03-1996	NONE	
US 5748783 A	05-05-1998	AU 6022396 A	29-11-1996
		CA 2218957 A	14-11-1996
		EP 1003324 A	24-05-2000
		EP 0824821 A	25-02-1998
		WO 9636163 A	14-11-1996
		US 5862260 A	19-01-1999
		US 5841886 A	24-11-1998