

申請日期: 89.10.19	案號: 89109631
類別: H04N 32	

(以上各欄由本局填註)

發明專利說明書

465224

一、發明名稱	中文	使用新穎水印介入和檢波方法之數位資料水印系統
	英文	DIGITAL DATA WATERMARKING SYSTEM USING NOVEL WATERMARK INSERTION AND DETECTION METHODS
二、發明人	姓名 (中文)	1. 弗羅恩 2. 杜哈美爾
	姓名 (英文)	1. Furon, Teddy 2. Duhamel, Pierre
	國籍	1. 法國 2. 法國
	住、居所	1. 法國勒恩市路德拉生特13號 2. 法國帕里西羅賓森市盧科堤25號
三、申請人	姓名 (名稱) (中文)	1. 法商·湯姆生多媒體公司
	姓名 (名稱) (英文)	1. THOMSON multimedia
	國籍	1. 法國
	住、居所 (事務所)	1. 法國布羅格比倫寇特市魁里加羅46號
	代表人姓名 (中文)	1. 建國漢
	代表人姓名 (英文)	1. ZHANG, Jianguo



本案已向

國(地區)申請專利

法國 FR

申請日期

1999/06/01 9907139

案號

主張優先權

有

有關微生物已寄存於

寄存日期

寄存號碼

無



五、發明說明 (1)

本發明係關於數位資料之水印領域。尤指一種水印系統，使用新穎水印介入和檢波方法，以及實施此等方法之裝置。

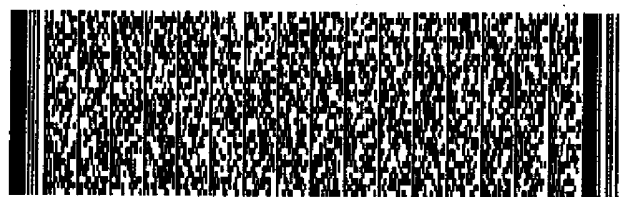
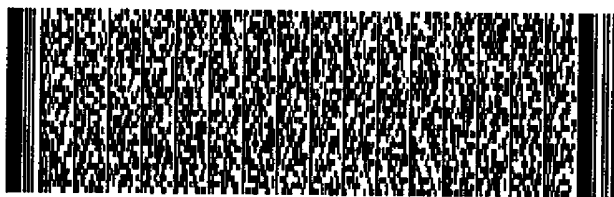
邇來對擅自拷貝數位資料之防護方法，是使用資料水印的原理，包含把印記項（通常稱為「水印」）以不知不覺方式介入於多媒質內容（靜像、視頻、聲頻等）。水印可例如為信號，表示內容不能拷貝，或為任何其他項，使多媒質內容供應者可以檢知不合法的拷貝。

為完美扮演其角色，水印必須抵擋得住有水印內容的轉型，不論轉型是由想抹消水印的私人刻意所為，或因含有水印資料的信號傳輸之際發生的失真所致。

習知技藝已知各種資料水印技術。特別參見EP-A-0 828 372、EP-A-0 840 513、WO-A-98/03014或WO-A-98/54897，記載水印介入所要防護資料之方法，以及資料內有該水印存在之檢波方法。

一般用來說明資料水印原理的方案如第1圖所示。第一組件1係關於把隱藏項W（水印）介入於要防護的內容C內。結果為有水印的內容CT。組件2係關於所接收內容CT內W項存在之檢測。另一資料K亦為水印介入和檢波方法所必須。此資料K必須以祕密方式由水印介入和檢波裝置共享，利用所謂對稱或私鍵密碼通信系統之類比，稱為鍵。

例如已知之水印技術包含，於要加水印的資料添加虛擬隨機雜訊順序。在此情況下，檢波法是藉實施相關計算進行，若與參攷虛擬雜訊順序（供水印介入之用）的相關，



五、發明說明 (2)

大於指定臨限值，即宣告所接收的資料有水印。在此例中，參攷虛擬雜訊順序即構成第1圖資料水印方案中的鍵K。

此方案的問題是可以檢測水印之各實體，必須共用同鍵K，一如介入水印之實體。在此情況下，能夠檢測水印的實體可以進一步加以刪除或修飾，因而放棄資料初期水印的全部益處。因此，受到水印防護的內容供應者，應與其鍵K通信，用來介入水印，而非以祕密方式至可信賴的實體。此舉在許多領域內大為限制使用資料水印之可能性。

具體言之，在消費者電子用具領域內，公知幾乎不可能在任何情況以合理成本，在用具內或該用具所含軟體內儲存祕密參變數。智慧卡被視為容許安全儲存祕密參變數的唯一設備，本身電力不足以進行連接水印檢波法之計算。

在上述實施例中，若係對要加水印的資料添加虛擬隨機雜訊順序，以進行加水印，即使參攷虛擬雜訊順序是祕密儲存在水印檢波裝置內，已證明過私人理論上可以發現參攷順序，因而藉觀察檢波器的輸出，做為大量不同輸入信號的函數，即可從資料刪除水印。

本發明旨在解決上述問題。

為達成此目的，本發明係關於水印在代表所要防護內容的資料內之介入方法。按照本發明，此方法包括步驟有：

(a)供應虛擬隨機雜訊順序至具有預定脈衝響應的濾



五、發明說明 (3)

波器之輸入；以及

(b)對資料添加濾波過的虛擬雜訊順序者。

按照本發明較佳要旨，此法又包括步驟為：

(c)在步驟(b)之前，進行資料之虛擬隨機交錯；和

(d)在步驟(b)之後，進行反向交錯，以獲得加水印之資料者。

本發明亦涉及一種在代表所接收內容之資料內的水印檢波方法，其特徵為，包括如下步驟：

(i)進行資料之光譜分析；和

(ii)由此推論是否資料含有虛擬雜訊順序，已利用具有預定光譜響應之濾波器加以濾波者。

按照本發明另一較佳要旨，所接收資料之虛擬隨機交錯，與上述步驟(c)所進行交錯一致，是在步驟(i)之前進行。

本發明亦涉及對資料加水印系統，使用上述水印介入方法和水印檢波方法。按照本發明，使用第一系列的參變數，私鍵，供水印介入，以及第二系列的參變數，公鍵，供水印檢波，故

一知道公鍵不可能知道私鍵；而

一知道檢波方法和公鍵，不可能刪除或修飾水印。

本發明又涉及在代表所要防護內容的資料內之水印介入裝置。按照本發明，此裝置包括：

一虛擬隨機雜訊順序之發生機構；

一具有預定脈衝響應之濾波機構，適於接收虛擬雜



五、發明說明 (4)

訊順序，並供應濾波後的虛擬雜訊順序；以及

一濾波後虛擬雜訊順序對資料之添加機構。

按照本發明較佳具體例，此裝置又包括：

一代表所要防護內容的資料虛擬隨機交錯之第一機構，以供應交錯資料，交錯資料係供應至加法機構，以便添加至濾波後的虛擬雜訊順序；以及

一第一交錯機構之反向交錯機構，連接至該加法機構之輸出，以供應加水印之資料者。

按照本發明特殊具體例，此裝置包括：

一轉型機構，把要防護的內容轉型為代表內容之資料；

一表示可添加於資料的雜訊最大量之調變順序發生機構；

一代表所要防護內容的資料虛擬隨機交錯之第一機構，以供應交錯之資料；

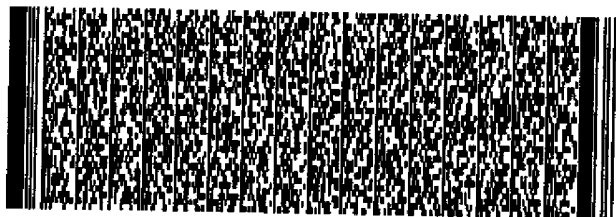
一虛擬隨機交錯的第二機構，與適於接收調變順序的第一機構，以供應交錯調變順序；

一乘法機構，適於一方面接收交錯調變順序，另一方面接收濾波過得虛擬雜訊順序，以供應水印；

一交錯資料和水印之加法機構，加法機構之輸出聯結於：

一第一和第二交錯機構之反向交錯機構，以供應加水印之資料；和

一加水印資料反向轉型為加印內容之機構。



五、發明說明 (5)

本發明亦涉及代表所接收內容的資料內水印檢波裝置。按照本發明，裝置包括：

- 一資料的電力光譜密度之評估機構；和
- 一假設之可能試驗機構，以評估是否資料包含已利用具有預定光譜響應的濾波器加以濾波過的虛擬雜訊順序。

按照特殊具體例，裝置又包括：

- 一代表所接收內容的資料之虛擬隨機交錯機構，適於進行與介入裝置的第一交錯機構同樣之交錯，交錯資料即供應至電力光譜密度之評估機構。

按照另一特殊具體例，此裝置又包括：

- 一把所接收內容轉型為代表內容的資料之機構，此轉型機構適於進行與介入裝置的轉型機構同樣之轉型。

本發明其他特徵和優點，由閱讀如下參照附圖所示特殊具體例之說明即可明白，惟本發明不限於此，附圖中：

第1圖已如前述，說明水印數位資料之已知方案；

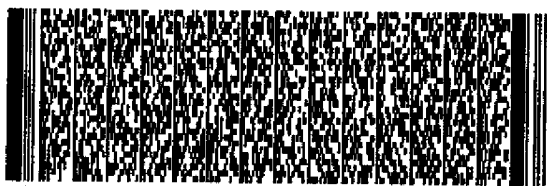
第2圖簡略表示本發明水印介入裝置；

第3圖簡略表示本發明水印檢波裝置；

第4圖表示本發明水印數位資料的新方案。

第2圖簡略表示本發明裝置，可供水印介入於代表要防護內容之信號內。此信號特別指數位視頻或聲頻信號，或另外代表照片等靜態影像或電腦計算的合成影像之信號，或更一般性是指代表多媒質內容之任何信號。

首先，要防護的內容是利用轉型模組10轉型為數位資



五、發明說明 (6)

料順序 $x = \{x_n\}$ ， n 在 1 和 N 之間。例如，若受防護的內容為包含 N 圖素的影像，則係數 x_n 可相當於影像各圖素的亮度。亦可為代表受防護內容的信號之離型傅立葉轉型係數，或傅立葉 - 梅林轉型係數，或受防護內容為靜態影像時，為小波分解係數。

資料順序 X 代表受防護的內容，一方面傳輸到模組 HPM 12，輸出調變順序 $m = \{m_n\}$ ， $\forall n \in [1..N]$ 。模組 HPM 計算此調變順序，做為根據人感受模式，諸如眼睛的 Sarnoff's 模式之演算函數。此順序 $m = \{m_n\}$ 代表最大量的雜訊，可加於各係數 x_n ，而無感受到品質的損失。

按照本發明一要旨，資料順序 x 又傳輸至交錯器 20，進行係數 x_n 的隨機排列 p ，以供應交錯係數順序 $\hat{x} = \{x_{p(n)}\}$ 。此項資料順序 x 交錯之目的隨後加以說明。

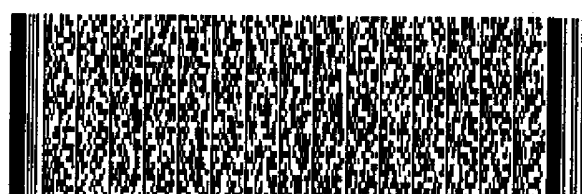
調變順序 m 亦傳輸至交錯器 14，進行和交錯器 12 所進行同樣係數 m_n 的排列 p ，以輸出交錯的調變順序 $\hat{m} = \{m_{p(n)}\}$ 。

為構成水印，以便介入於代表受防護內容的資料順序 x 內，虛擬隨機雜訊發生器（圖上未示）先供應虛擬雜訊順序 $v = \{v_n\}$ ， $\forall n \in [1..N]$ ，具有高士分佈。此虛擬雜訊順序 v 傳輸至線性時定 (LTI) 型濾波器 16 之輸入，其脈衝響應為：

$$h = \{h_n\}, \forall n \in [1..L]$$

其中 L 為相當於濾波器長度之整數；其光譜響應為 $H(f)$ ， $H(f)$ 係 h 的傅立葉轉型。

在濾波器 16 的輸出，可得濾波的虛擬雜訊順序 $w = \{w_n\}$ ， $\forall n \in [1..N]$ ，滿足下式 (1)：



五、發明說明 (7)

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

其中代表迴旋乘積。

由此，從干擾導衍出以下二式(2)和(3)：

$$\phi_{ww}(\tau) = (h \otimes h) \otimes \phi_{vv}(\tau) \quad (2)$$

其中 $\phi_{ww}(\tau)$ 和 $\phi_{vv}(\tau)$ 分別代表 w 和 v 的自生相關函數；以及

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

其中 $\Phi_{ww}(f)$ 和 $\Phi_{vv}(f)$ 分別代表 $\phi_{ww}(\tau)$ 和 $\phi_{vv}(\tau)$ 的電力光譜密度，亦即其傅立葉轉型。

由於 v 是具有高士分佈的虛擬隨機雜訊順序，其光譜亦即函數 $\Phi_{vv}(f)$ 具有實質上平坦形狀。另方面，一旦此順序 v 被濾波器 16 所濾波，則所得順序 w 顯示光譜 $\Phi_{ww}(f)$ ，就 $|H(f)|^2$ 項而言不再平坦。另外重要的是注意到（可以理解本發明之其餘），知道（同理，知道 $H(f): |H(f)|$ 的模組）不能檢索 $H(f)$ （和 h ），因為對 $H(f)$ 相有不確定性。

回到第 2 圖，濾波過的虛擬雜訊順序 w 乘以交錯調變順序 $\hat{x}$ （倍增器 18），而所得構成水印之順序，即加於交錯資料順序 $\hat{x}$ （加算器 22）。

加算器 22 的輸出順序指明 $\hat{y} = \{y_{p(n)}\}$ ，並滿足下式(4)和(5)：

五、發明說明 (8)

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

$$\tilde{y} = \tilde{x} + \tilde{m} \cdot (h \otimes v) \quad (5)$$

加水印交錯資料順序 $\hat{y}$ 之電力光譜密度，由下式(6)和(7)賦予：

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

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

在式(7)中， μ_j 和 σ_j 分別代表順序 $j = \{j_n\}$ 的平均和標準偏差，其 $j \in \{x, m, v\}$ ， $\delta(f)$ 相當於狄悅克脈波，而

$\left(\sigma_m^2 \cdot \sigma_v^2 \cdot \sum_u h_u^2 \right)$ 項等於常數。

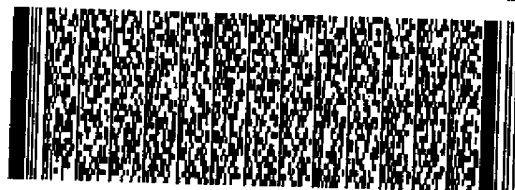
加水印交錯資料順序 $\hat{y}$ 再傳輸至反向交錯器24，進行與交錯器20和14所進行排列 p 相反的操作，以供應加水印資料順序 $y = \{y_n\}$ ，其係數與資料 $x = \{x_n\}$ 的初階同階。

再由模組26進行轉型模組10所進行相反的轉型，以獲得加印內容(或加水印內容)，因而可防止擅自拷貝，內容感受不到水印。

茲參見第3圖說明所接收內容的水印檢波裝置，此水印已介入於諸如第2圖所示裝置防護之內容。

檢波原理是根據所接收信號的光譜分析。

所接收信號代表尋求決定是否為加水印之接收內容。此內容與前述要防護的內容同型。在以下例中，假設所接收內容為含 N 圖素之影像。



五、發明說明 (9)

所接收內容先傳輸至轉型模組30，進行和第2圖水印介入裝置的模組10同樣轉型操作，以供應代表所接收內容之資料順序 $r = \{r_n\}$, $\forall n \in [1..N]$ 。在本案例中，假設所接收影像的圖素所得亮度 r_n ，做為轉型模組30之輸出。

若所接收內容正確相當於第2圖裝置發出的加水印內容，意即若在水印介入裝置和檢波裝置之間傳輸當中，未發生轉型或信號失真，則可得：

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

實際上，並非始終如此，因為在傳輸之際，信號有時會進行轉型。

由於在第2圖裝置內，水印已介入於交錯資料順序 $\hat{x}$ 內，為檢測所接收內容中可能有水印存在，資料順序 r 可傳輸至交錯器32，進行和第2圖交錯器20和14所進行係數 r_n 之同樣排列 p 。

得交錯資料順序 $\hat{r} = \{r_{p(n)}\}$ ，做為交錯器32之輸出。

先前已知若介入之水印，係具有脈衝響應 h 和光譜響應 $H(f)$ 的濾波器所濾波過的虛擬雜訊順序，則所得(交錯)資料順序 $\hat{y}$ 的電力光譜密度，以關係式(6)和(7)表示。

資料順序 x 和調變順序 m 的交錯目的，如今已明顯。當然，如果資料順序 x 代表影像的圖素，其光譜密度具有幅度差異很大的非常結構化形狀。資料的交錯任務，在於切斷此順序的統計上的連貫性，故交錯資料順序 $\hat{x}$ 的光譜密度具有實質上平坦形狀，一如具有高士分佈之虛擬雜訊順序。



五、發明說明 (10)

因此，如果於此交錯順序加水印，係由具有光譜響應 $H(f)$ 的濾波器所濾波過的虛擬雜訊順序，則所得資料順序，其電力光譜密度可由關係式(7)表示，其中可檢知重要項 $|H(f)|^2$ 。

所以，檢波原理是根據順序 $\tilde{r}$ 的光譜分析以及最大可能比率假設測試 (MLR 假設測試)，所測試假設如下：如果交錯資料順序 $\tilde{r}$ 含有雜訊，是否為利用其光譜響應具有類似 $|H(f)|$ 模組的濾波器濾波過的雜訊？若響應為是，可由此推論出順序 $\tilde{r}$ 內存在的雜訊為水印，而在相反情況下，可由此得出結論，即所接收內容未加水印。

實際上，此項分析是根據有關光譜分析和可能的假設測試之計算，詳見 K. Dzhaparidze 著作《靜態時系的光譜分析中之參變數估算和假設測試》，Springer 統計叢書，Springer 出版社，1986 年出版，進一步細節可以參攷此書。

回到第 3 圖，所接收交錯資料順序 $\tilde{r}$ 傳輸至模組 34，進行 Periodogram 微積分。此項微積分旨在估算順序 $\tilde{r}$ 的電力光譜密度。在輸出可得如下關係式(8)賦予之量 $I_N(f)$ ：

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

此量再傳輸至模組 36，進行 MLR 假設測試，以決定所接收內容加水印 (輸出響應 Y) 與否 (輸出響應 N)。

模組 36 測試二種假設的可能性：

一按照第一種假設 G_0 ，所接收內容未加水印，因而

五、發明說明 (11)

順序 $\hat{r}$ 之光譜密度實質上平坦，可經由如下關係式 (9) 加以估算：

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

一按照第二種假設 G_1 ，所接收內容加水印，而順序 $\hat{r}$ 之光譜密度可經由如下關係式 (10) 估算：

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

其中 C 為常數， σ_v 等於 1 (選擇虛擬雜訊順序 v 宜在介入裝置的水準，使 σ_v 等於 1，但亦可同樣選擇其他數值)。此外， μ_m 基準在介入裝置的水準，等於例如 3。

為估算假設 G_0 和 G_1 ，模組 36 按照下列關係式 (11) 計算二數 $U_{N,0}(\hat{r})$ 和 $U_{N,1}(\hat{r})$ ，代表假設 G_0 和 G_1 之可能性：

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

比較此二數，模組 36 可由此推論：

一若 $U_{N,1}(\hat{r}) > U_{N,0}(\hat{r})$ ，則檢波器的響應為 Y ，意即所接收的內容加水印；而

一若 $U_{N,1}(\hat{r}) < U_{N,0}(\hat{r})$ ，則檢波器的響應為 N ，意即所接收的內容未加水印。

亦可以較佳方式計算差值 $(U_{N,1}(\hat{r}) - U_{N,0}(\hat{r}))$ ，若此差值大於預定臨限值，並進行上述比較，以保證檢波有更佳準確性。

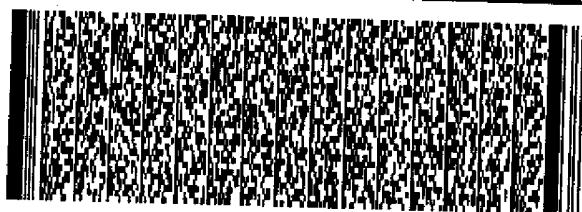
五、發明說明 (12)

參見第2和3圖說明如上之水印介入和檢波方法，可產生新穎的水印系統，如第4圖所示。在此新穎系統中，並按照本發明較佳要旨，使用稱為「私鍵」 K_{PRI} 的參變數，把水印 W 介入(100)於內容 C 中，而使用稱為「公鍵」 K_{PUB} 的另一參變數，供檢測(200)所接收內容 CT 中的水印。「私鍵」和「公鍵」項的使用，可類比公鍵密碼使用系統。須知此處的水印 W 係二進位，意即不論內容 C 加水印與否， W 都不含其本身任何項目。

在上述具體例中，私鍵 K_{PRI} 是由虛擬隨機雜訊順序 v 以及濾波器16的脈衝響應 h 所形成(第2圖)。順序 $v=\{v_n\}$ 和 $h=\{h_n\}$ 實際上對順序 $w=\{w_n\}$ 的計算是不可或缺，此順序 w 本身在乘以交錯調變順序 $\hat{m}$ 後，介入於代表要防護內容的資料內。

用來檢測所接收內容中水印的公鍵，係由濾波器16光譜響應的模組 $|H(f)|$ 所形成。當然，在檢測所接收內容 CT 中水印存在所進行之光譜分析計算(第3圖之模組34和36)中，只有知道 $|H(f)|$ 是必要的。具體言之，不必要知道 v 和 h (私鍵)來進行水印之檢波。實際上，如前述可見知道 $|H(f)|$ 不足以知道 $H(f)$ 和 h 。

因此，可得一系統，知道公鍵不可能由此推論私鍵。又，不知私鍵則不可能使裝置進行水印檢波加以刪除或修飾。是故，可在非安全環境內進行檢波，而無抹消水印之虞。



圖式簡單說明

- 第1圖已如前述，說明水印數位資料之已知方案；
第2圖簡略表示本發明水印介入裝置；
第3圖簡略表示本發明水印檢波裝置；
第4圖表示本發明水印數位資料的新方案。



四、中文發明摘要 (發明之名稱：使用新穎水印介入和檢波方法之數位資料水印系統)

水印系統使用第一系列參變數(v, h)，私鍵(K_{PRI})，以供水印介入，以及第二系列參變數($|H(f)|$)，公鍵(K_{PUB})，以供水印檢波，故公鍵的知識不能知道私鍵，且不能刪除或修飾水印。

水印的介入是對要加水印的資料，添加虛擬隨機雜訊順序(v)進行，利用具有脈衝響應(h)的濾波器加以濾波。

水印的檢波是就所接收資料查尋，看是否含有以具有預定光譜響應($H(f)$)的濾波器濾波過的雜訊。

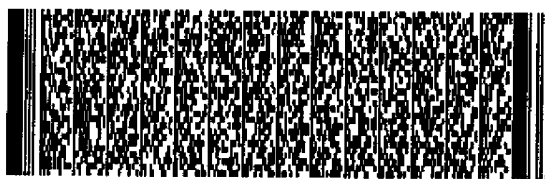
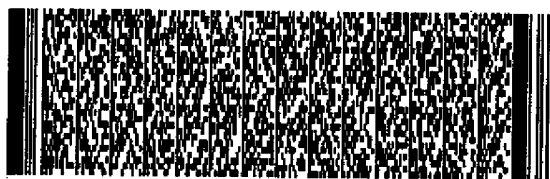
應用於防拷貝。

(第4圖)

英文發明摘要 (發明之名稱：DIGITAL DATA WATERMARKING SYSTEM USING NOVEL WATERMARK INSERTION AND DETECTION METHODS)

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),



四、中文發明摘要 (發明之名稱：使用新穎水印介入和檢波方法之數位資料水印系統)

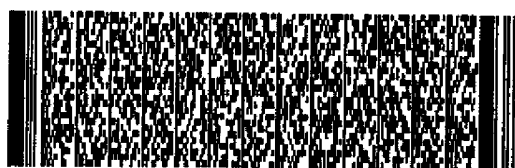
英文發明摘要 (發明之名稱：DIGITAL DATA WATERMARKING SYSTEM USING NOVEL WATERMARK INSERTION AND DETECTION METHODS)

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.

(Figure 4)



六、申請專利範圍

1. 一種水印介入於代表所要防護內容的資料(x)內之方法，其特徵為，包括下列步驟：

(a)對具有預定脈衝響應(h)的濾波器輸入，供應虛擬隨機雜訊順序(v)；和

(b)對該資料加該濾波過之虛擬雜訊順序(w)者。

2. 如申請專利範圍第1項之方法，其中又包括下列步驟：

(c)在步驟(b)之前，進行資料(x)之虛擬隨機交錯(p)；和

(d)在步驟之後，進行反向交錯，以獲得加水印之資料者。

3. 一種在代表所接收內容之資料(r)內的水印檢波方法，其特徵為，包括如下步驟：

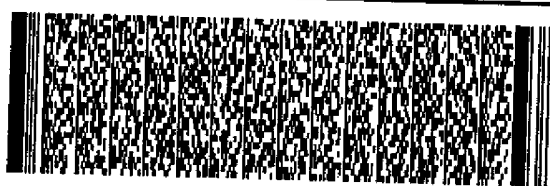
(i)進行該資料之光譜分析；和

(ii)由此推論該資料是否含有已經利用具備預定光譜響應($H(f)$)的濾波器濾波過的虛擬雜訊順序者。

4. 如申請專利範圍第3項之方法，供檢測在代表所接收內容的資料(r)中之水印，水印係適於按照申請專利範圍第2項之方法介入，其中又包括下列步驟：

(iii)在步驟(i)之前，進行所接收資料(r)之虛擬隨機交錯(p)，與步驟(c)進行之交錯一致者。

5. 一種水印系統，使用申請專利範圍第1或2項之一的水印介入方法，以及申請專利範圍第3或4項之一的水印檢波方法，其特徵為，使用第一系列的參變數(v, h)，即私



六、申請專利範圍

鍵(K_{PRI})，以介入水印，並使用第二系列的參變數($|H(f)|$)，即公鍵(K_{PUB})，對水印檢波，故：

- 一知道公鍵不可能知道私鍵，而
- 一知道水印檢波方法和公鍵，不可能刪除或修飾水印者。

6. 一種水印介入於代表所要防護內容的資料(x)內之裝置，其特徵為，包括：

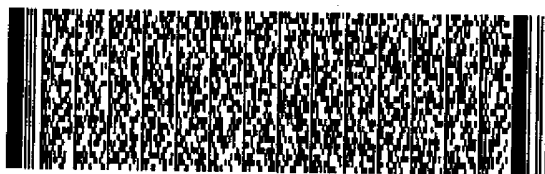
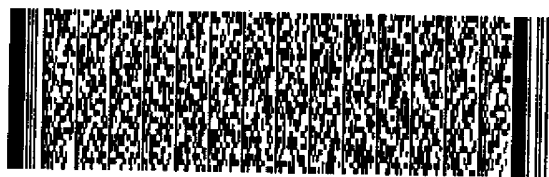
- 一虛擬隨機雜訊順序(v)之發生機構；
- 一濾波機構(16)，具有預定脈衝響應(h)，適於接收該虛擬雜訊順序(v)，以及供應濾波過的虛擬雜訊順序(w)；和
- 一對該資料(x)加該濾波過的虛擬雜訊順序(w)所用之機構者。

7. 如申請專利範圍第6項之裝置，又包括：

- 一代表所要防護內容的資料(x)虛擬隨機交錯之第一機構(20)，以供應交錯資料($\hat{x}$)，該交錯資料係供應至加法機構(22)，以便加於濾波過的虛擬雜訊順序(w)；和
- 一該第一交錯機構(20)之反向交錯機構(24)，聯結至該加算機構(22)之輸出，以供應加水印之資料者。

8. 如申請專利範圍第6項之裝置，又包括：

- 一所要防護的內容轉型為代表該內容的資料(x)所用之機構；
- 一調變順序(m)之發生機構(12)，表示可加於該資料之最大雜訊量；



六、申請專利範圍

其特徵為，又包括：

— 代表所要防護內容的該資料(x)虛擬隨機交錯之第一機構(20)，以供應交錯資料($\hat{x}$)；

— 虛擬隨機交錯之第二機構(14)，與第一機構(20)一致，適於接收該調變順序(m)，以供應交錯調變順序($\hat{m}$)；

— 乘法機構(18)，適於一方面接收交錯調變順序($\hat{m}$)，另方面接收濾波過的虛擬雜訊順序(w)，以便供應水印；

— 交錯資料($\hat{x}$)和水印之加法機構(22)，該加法機構之輸出係聯結至：

— 該第一(20)和第二(14)交錯機構之反向交錯機構(24)，以供應加水印資料(y)；以及

— 加水印資料反向轉型為加印內容之機構(26)者。

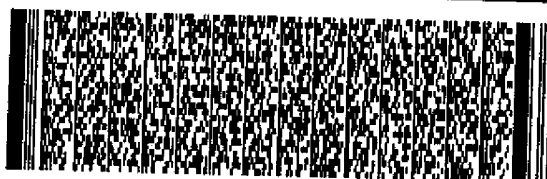
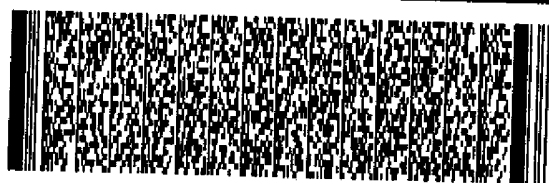
9. 一種代表所接收內容的資料(r)中水印之檢波裝置，包括：

— 該資料的電力光譜密度之評估機構(34)，和

— 假設的可能性測試機構(36)，以評估該資料是否含有已經利用具有預定光譜響應($H(f)$)的濾波器加以濾波過之虛擬雜訊順序者。

10. 如申請專利範圍第9項之裝置，適用於按照申請專利範圍第7或8項介入裝置所介入水印之檢波，包括：

— 代表所接收內容的資料(r)之虛擬隨機交錯機構(32)，適於進行與介入裝置之該第一交錯機構(20)的同樣



六、申請專利範圍

交錯，該交錯過的資料($\hat{r}$)係供應至該電力光譜密度之評估機構(34)者。

11. 如申請專利範圍第10項之裝置，適用於按照申請專利範圍第8項介入裝置所介入水印之檢波，其中又包括：

一所接收內容轉型為代表該內容的資料(r)所用之機構(30)，該轉型係適於進行與介入裝置的轉型機構(10)之同樣轉型者。



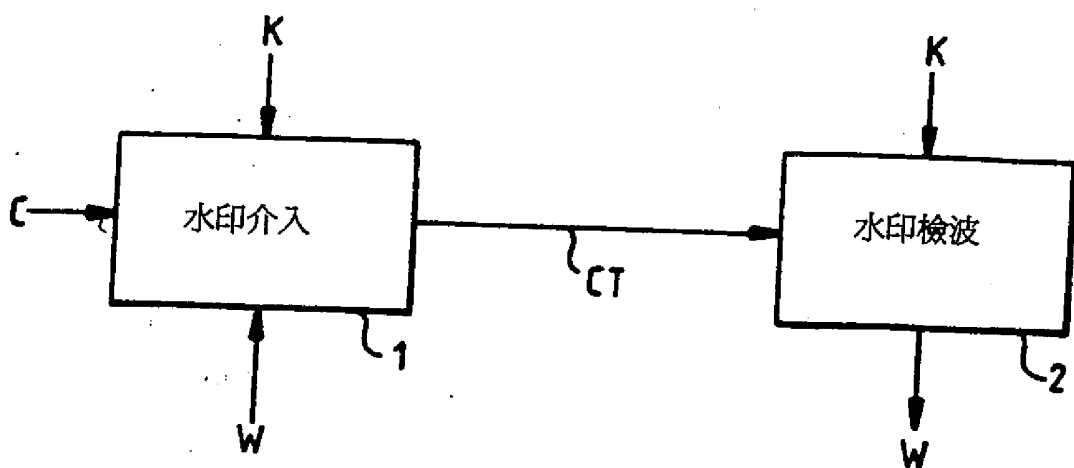


圖 1

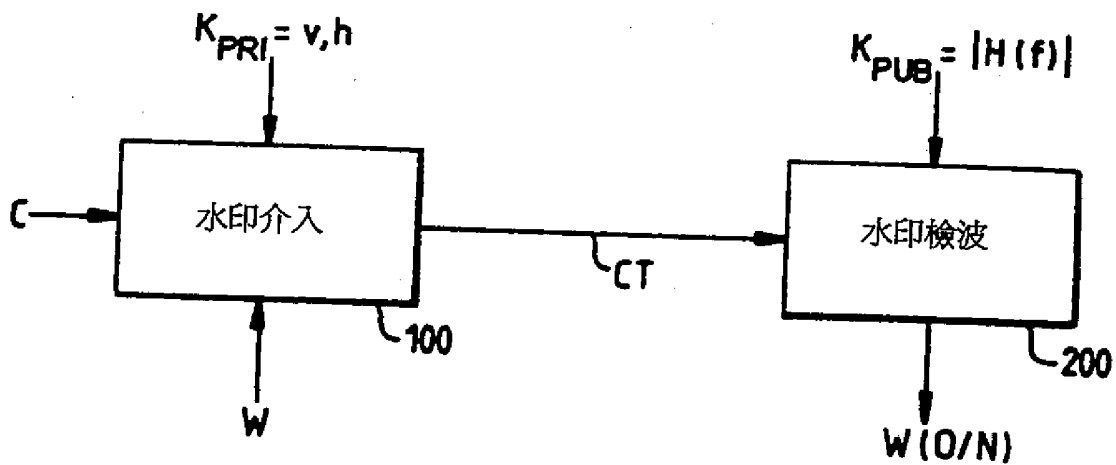


圖 4

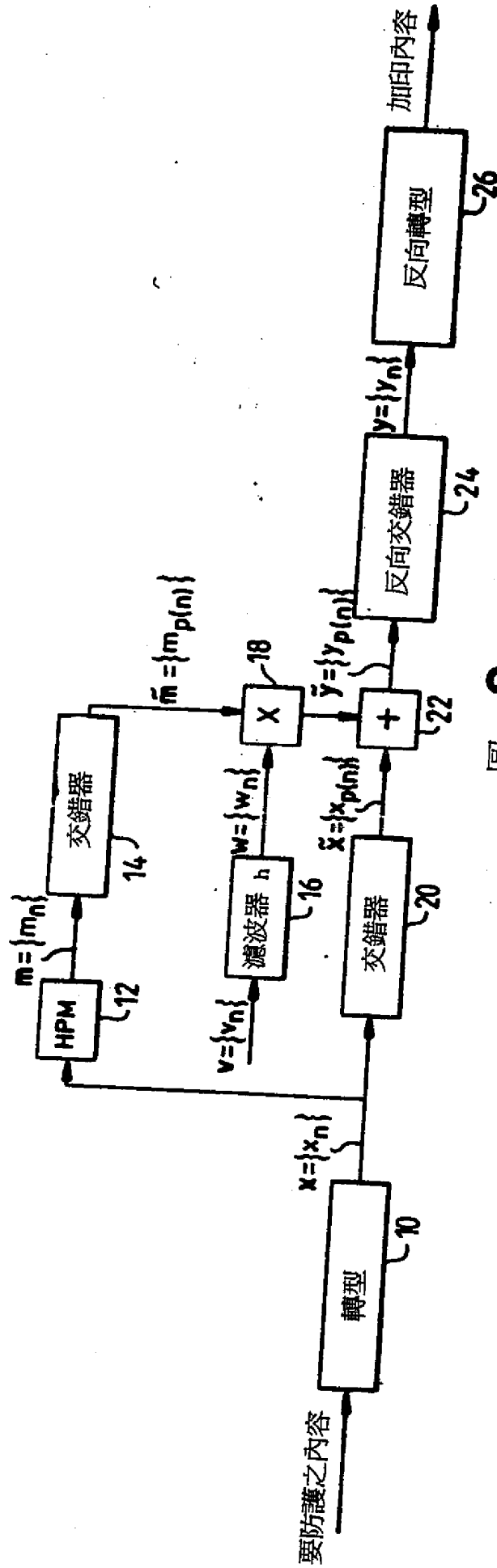


圖 2

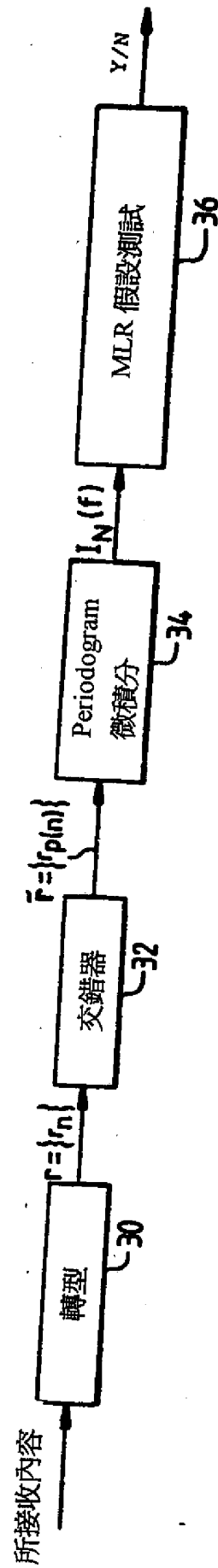


圖 3