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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 December 2006 (07.12.2006)

PCT

(10) International Publication Number
WO 2006/129293 A1

(51) International Patent Classification:
G10L 19/00 (2006.01) *H04N 7/26* (2006.01)
G06T 1/00 (2006.01)

(21) International Application Number:
PCT/IB2006/051773

(22) International Filing Date: 2 June 2006 (02.06.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
05104828.8 3 June 2005 (03.06.2005) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **LEMMA, Aweke, N.** [NL/NL]; C/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **VAN DER VEEN, Minne** [NL/NL]; C/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **TUYLS, Pim, T.** [BE/BE]; C/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **KALKER, Antonius, A., C., M.** [NL/US]; C/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agents: **SCHMITZ, Herman, J., R.** et al.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

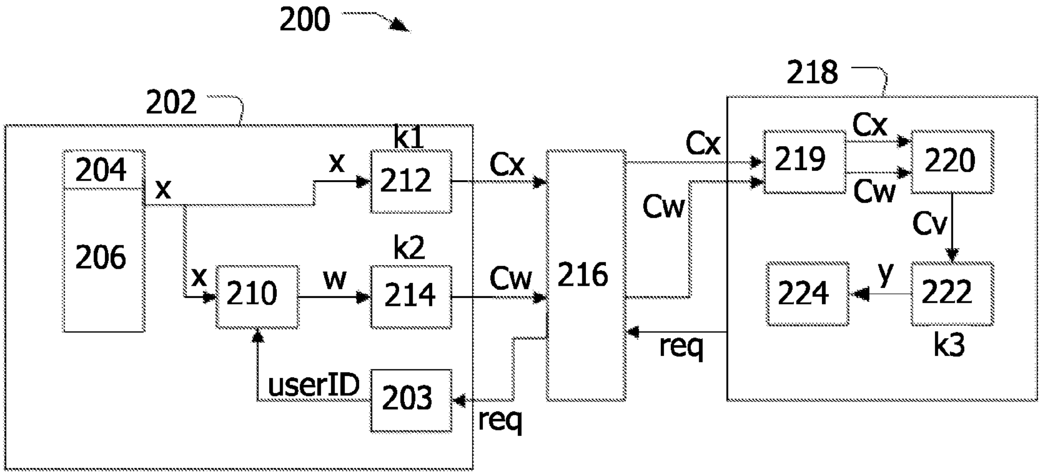
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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:** HOMOMORPHIC ENCRYPTION FOR SECURE WATERMARKING



(57) **Abstract:** A method and a system for embedding a watermark in a media signal x are disclosed. The method comprises providing an at least partially encrypted media signal c_x of said media signal x, wherein encryption is performed using a first encryption key k1; providing an at least partially encrypted watermark signal c_w, wherein encryption is performed using a second encryption key k2; combining the at least partially encrypted media signal c_x and the at least partially encrypted watermark signal c_w in a combiner to obtain an encrypted combined media signal c_y; and obtaining a decrypted watermarked media signal y by decrypting said encrypted combined media signal c_y using a third decryption key k3. The present invention provides a framework for secure watermark embedding within untrusted devices.

Homomorphic encryption for secure watermarking

Field of the Invention

This invention pertains in general to the field of secure transmission of data. More particularly the invention relates to a method and arrangement for embedding a watermark in a media signal in an electronic music delivery system and more particularly to homomorphic encryption for secure watermarking in an electronic music delivery system.

Background of the Invention

A conventional electronic music distribution (EMD) system 100 for distributing music data is illustrated in Fig. 1. The EMD system 100 comprises a server 102, a client 118 and a distribution network 116 such as the Internet. In general, the server 102 encrypts content data and content information such as copyright information by using session key data obtained after performing mutual authentication between the content provider and a user who has requested the content via the distribution network 116. The encrypted information is transferred to the client 118 who then decrypts the encrypted information to obtain the requested content.

More specifically, after the request for content, sent from the client 118 to the server 102 via the network 116, has been authenticated, the content provider 104 sends the requested content 106 to a watermark engine 110 and sends the content information 108 to a payload device 112. The content information 108 may include serial copy management system (SCMS) information, digital watermark information for embedding copyright information into the content data and information for embedding copyright information into transmission protocols of the server 102.

The payload device 112 computes the appropriate payload to be embedded and transfers the payload pL to the watermark engine 110. The watermark engine embeds the payload pL into the content 106. The combined data from the watermark engine 110 is then encrypted by an encryption device 114. The combined data is conventionally encrypted by a single encryption key. The encrypted signal E(y) is then sent to the client 118 over the Internet 116. The client 118 then decrypts the encrypted signal E(y) in a decryption device

120. The watermarked but decrypted content is then stored in a user database 122 for use by the user.

Presently, the server processes run at about 40 times real time on a 3 GHz Pentium IV processor. Though this is acceptable in many instances, it may not be sufficient for mass content distribution requiring millions of simultaneous accesses. In this case, a fixed low complexity server is desirable with the possibility for multi-casting and caching. These and other features desired to have implemented, such as service flexibility, can be achieved if the watermark embedding is done at the client side. Generally however, client side embedding will make the watermarking system vulnerable to hacking and should therefore be avoided. Particularly, if the client is allowed to possess both the watermarked and non-watermarked contents, it is extremely easy to maliciously remove or modify the watermark and even to estimate the underlying algorithm. In conclusion, there is a need for a client-side embedding that is implemented by providing a cryptographically secure embedding solution.

One solution for secure watermark embedding, also referred to as watercrypt, is disclosed in "Large scale distributed watermarking of multicast media through encryption" by Roland Parviainen and Peter Parnes, presented at the CMS2001 conference, Darmstadt, Germany. The idea there is to have two encrypted media streams x_1 and x_2, equipped with watermarks w_1 and w_2, respectively. Encryption and watermarking is done on a frame-by-frame (packet) basis, i.e. having one packet it is possible to extract either watermark w_1 or w_2. Every packet is encrypted with a different key K_e[i]. Therefore, a total of 2k random encryption keys K_e[1], K_e [2], …, K_e [2k] is required. Both x_1 and x_2 are transmitted to every user.

Each user is given a unique sequence of decryption keys K_d[i] which determines the sequence in which the signals x_1 and x_2 are decrypted. If x_1 and x_2 are encoded as binary "0" and "1", a total of N=k bit information can be carried with such a watermark. The shortcoming of this approach is that two parties can easily combine two decrypted sequences, just by concatenating alternating segments, to generate either invalid payload or a new valid payload pointing to another client. Such an attack can compromise the entire system and makes the algorithm inapplicable to applications such as EMD.

Another framework that can be used for embedding a watermark in a secure domain is disclosed in "Processing Encrypted Data" by Niv Ahituv, Yeheskel Lapid, and Seev Neumann, Communications of the ACM, Volume 30 no. 9, 1987. In this article, an idea of processing encrypted data for the purpose of updating the balance of certain bank accounts by subtraction or addition is discussed. They suggest to use homomorphic encryption functions satisfying the rules:

$$E_{k1,k2}(A+B)= E_{k1}(A)+ E_{k2}(B), \text{ and}$$

$$E_k(axB)= E_k(A)x\ a.$$

This solution however lacks an actual implementation based on specific algorithms. Moreover, the disclosed method assumes a modulo arithmetic and does not work under overflow conditions.

Hence, an improved method for embedding watermarks would be advantageous and in particular a method and system allowing for securely embedding a watermark at the un-trusted client-side of a distribution system would be advantageous.

Summary of the Invention

Accordingly, the present invention preferably seeks to mitigate, alleviate or eliminate one or more of the above-identified deficiencies in the art and disadvantages singly or in any combination and solves at least the above mentioned problems, at least partly, by providing a device, a method, a computer-readable medium, and a media signal that securely embeds a watermark at the client side of a distribution system, according to the appended patent claims.

The general solution according to the invention provides a framework for secure watermark embedding within un-trusted devices.

According to aspects of the invention, a method, an apparatus, and a computer-readable medium for embedding a watermark in a media signal in a device are disclosed.

According to one aspect of the invention, a method is provided for embedding a watermark in a media signal in a device. The method comprises: providing an at least partially encrypted media signal of the media signal, wherein encryption is performed using a first encryption key k1; providing an at least partially encrypted watermark signal, wherein encryption is performed using a second encryption key k2; combining the at least partially encrypted media signal and the at least partially encrypted watermark signal in a combiner to obtain an encrypted combined media signal; and obtaining a decrypted media signal by decrypting said encrypted combined media signal using a third decryption key k3.

According to another aspect of the invention, a system is provided for embedding a watermark in a media signal in a device. The system comprises: means for providing an at least partially encrypted media signal of the media signal, wherein encryption is performed using a first encryption key k1; means for providing an at least partially encrypted watermark signal, wherein encryption is performed using a second encryption key k2; means for combining the at least partially encrypted media signal and the at least partially encrypted watermark signal in a combiner to obtain an encrypted combined media signal; and means for obtaining a decrypted media signal by decrypting said encrypted combined media signal using a third decryption key k3.

According to a further aspect of the invention, a computer-readable medium having embodied thereon a computer program for embedding a watermark in media signal in a device, for processing by a computer is provided. The computer program comprises: a first code segment for providing an at least partially encrypted media signal of said media signal, wherein encryption is performed using a first encryption key k1; a second code segment for providing an at least partially encrypted watermark signal, wherein encryption is performed using a second encryption key k2; a third code segment for combining the at least partially encrypted media signal and the at least partially encrypted watermark signal in a combiner to obtain an encrypted combined media signal; and a fourth code segment for obtaining a decrypted watermarked media signal y by decrypting said encrypted combined media signal using a third decryption key k3.

According to yet another aspect of the invention, a media signal is provided. More specifically, an encrypted combined media signal is provided, comprising in combination an at least partially encrypted media signal of a media signal, wherein encryption is performed using a first encryption key k1, and an at least partially encrypted watermark signal, wherein encryption is performed using a second encryption key k2; wherein said combination signal is decryptable in order to provide a decrypted media signal by decrypting said encrypted combined media signal using a third decryption key k3, such that said media signal has a decrypted watermark embedded therein.

The present invention has at least the advantage over the prior art that it allows for the content to be watermarked at the client-side of a distribution system without the risk of the client being able to remove the watermark from the content received by the client, even if the client is untrusted.

Brief Description of the Drawings

These and other aspects, features and advantages of which the invention is capable of will be apparent and elucidated from the following description of embodiments of the present invention, reference being made to the accompanying drawings, in which

Fig. 1 is a schematic diagram of a known electronic music delivery system;

Fig. 2 is a schematic diagram of an electronic music delivery system according to one embodiment of the invention;

Fig. 3 is a flow chart illustrating homomorphic cryptography using the Paillier method according to another embodiment of the invention;

Fig. 4 is a flow chart illustrating homomorphic cryptography using the El Gamal method according to yet another embodiment of the invention; and

Fig. 5 illustrates a computer readable medium according to a further embodiment of the invention.

Description of embodiments

The following description focuses on a embodiments of the present invention applicable to an electronic music delivery system. However, it will be appreciated that the invention is not limited to this application but may be applied to many other distribution systems which employ watermarking techniques, e.g. image databases or the like.

Figure 2 illustrates the basic architecture of an electronic music delivery (EMD) system 200 according to one embodiment of the invention. Although the solution discussed hereafter is based on the EMD architecture of Figure 2, the same principle can also be applied to many other applications. In the EMD context, we make the following assumptions. We have a media distribution service consisting of a server and a client. The server is trusted and the client is not trusted. The client should not have access to non-watermarked content nor the watermark signal. The invention is of course applicable to all systems fulfilling similar assumptions.

The EMD system 200 comprises, among other features, a server 202, a client 218, and a distribution network 216 such as the Internet. When the client 218 wants to request content from a content provider, the client sends a request req to the server 202 over the network 216. For instance, the client 218 is an device for playing electronic music or video, for instance accessible via files in e.g. MP3 format, and the device, e.g. initiated by its user, requests a certain piece of music offered by a provider controlling server 202. A management processor 203 receives this request and authenticates the request in a known manner, for instance to ensure that the correct user is identified and/or debited for the subsequent download of the piece of music. Once authenticated, the content provider 204 sends the requested content 206, here in the form of a media signal x, to an encryption device 212. The encryption device 212 at least partially encrypts the content 206 using a first encryption key k_1, giving an at least partially encrypted media signal c_x. In addition, the content provider 204 also sends the content information (media signal x) for the requested content to a watermark engine 210. The watermark engine 210 takes the content information and the userID from the requesting user and computes the appropriate payload to be embedded. The payload information signal *w* is then sent to an encryption device 214. The encryption device 214 then encrypts the payload information signal *w* at least partly using a second encryption key k_2, resulting in a partially encrypted watermark signal c_w. As will be described in more detail below, the server 202 can use a variety of methods for encrypting the content and the payload information. For instance, instead of using two encryption modules, the server 202 may use a single encryption device with at least two encryption keys. The server 202 then transmits the at least partially encrypted content c_x and the at least partially encrypted watermark information signal c_w to the client 218 over the network 216, in an at least partially encrypted form, i.e. in a secure way.

The signals c_x and c_w are received by a receiver 219 and are then combined in a watermark engine 220. The two at least partially encrypted signals c_x and c_w are combined to generate a watermarked content in the encrypted domain. In other words, the client side watermark engine 220 performs the operation $c_y = \text{combine}\ (c_x, c_w)$.

The watermarked content c_y is then decrypted in a decryption device 222 using a third decryption key k_3. The decrypted data y from the decryption device 222 is the watermarked content only, i.e. the decrypted watermarked media signal y is generated by decrypting the encrypted combined media signal c_y using a third decryption key k3. The transmitted signal components x and w cannot be accessed by the client using the third decryption key k_3. As the user only has the key k3 to his disposal, he cannot manipulate the watermark, as components x and w are encrypted with k1 and k2, respectively, which are different from k3. However, decrypted signal y is a regular media signal that is watermarked and may be processed in a conventional way, e.g. in a user player unit 224.

According to another embodiment of the invention, the encryption and decryption of the content and payload information will now be described using homomorphic cryptography using the Paillier method. Figure 3 is a flow chart illustrating the homomorphic cryptography according to this embodiment of the invention. At the trusted server 202, the management processor 203, for example, selects two prime numbers p and q in step 302 and derives K=pq, N=LCM(p-1,q-1) where LCM is the least common multiplier in step 304. K and N are then supplied to the client 318. The management processor 203 then arbitrarily splits K as K=k1+k2 in step 306. For a positive integer r < K, the encryption device 212 now computes the at least partially encrypted content signal c_x where

$$c_x = (1+K)^x r^{k1} \bmod K^2 \text{ or} \tag{1}$$

$$c_x = (1+K)^x r^{N.k1} \bmod K^2 \tag{2}$$

in step 308. The encryption device 214 also computes the encrypted payload information signal c_w where $c_w = (1+N)^w r^{k2} \bmod K^2$ or $c_w = (1+N)^w r^{N.k1} \bmod K^2$ in step 310.

After c_x and c_w are transmitted to the client 218 over the network 216, the client 218 combines c_x and c_w where $c = c_w \cdot c_x = (1+N)^{w+x} r^{k1+k2} \bmod K^2$ in step 312. The client 218 then uses the decryption key k3=K supplied to him to extract the watermarked content in step 314 using

$$y = \frac{(c^N - 1) \bmod k3^2}{Nk3} \bmod k3 \quad \text{or} \quad y = \frac{(c-1) \bmod k3^2}{k3} \bmod k3 \tag{3}$$

Note that the relation given in (3) is a consequence of the following discrete mathematics identities. Given prime numbers p and q such that k3=p.q and N=LCM(p-1,q-1)

for any r<k3, $r^{NK} \bmod k3^2 = 1 \bmod k3^2$ and

for any integer a < k3, $(1+k3)^a \bmod k3^2 = (1+k3a) \bmod k3^2$.

Thus, depending on the definition of c_x in (1) and (2) c^N-1 mod $k3^2$ = $(1+N)^{N(x+x)} r^{Nk3} \bmod k3^2 = (1+Nk3(x+w)) \bmod k3^2$ or c-1 mod $k3^2 = (1+N)^{(x+x)} r^{Nk3} \bmod k3^2$ = $(1+k3(x+w)) \bmod k3^2$. Putting this into (3), we get

$$y = \frac{(c^N - 1) \bmod k3^2}{Nk3} \bmod k3 = (x+w) \bmod k3 \qquad \text{OR}$$

$$y = \frac{(c-1) \bmod k3^2}{k3} \bmod k3 = (x+w) \bmod k3 \tag{4}$$

If x+w < k3, then (x+w) mod k3 = x+w. Thus the client can decrypt the watermarked content. Since the client 218 does not know how k3 is split into k1 and k2, the client 218 can not decrypt the encrypted content signal and the encrypted payload information signal. In addition, the encrypted content signal can be broadcast. Each client (i) is then assigned a unique k2 (i.e., unique k3). The encrypted payload information signal is thus encrypted with this unique k2 so that only the client to whom the watermark is intended can decrypt x+w.

According to another embodiment of the invention, the encryption and decryption of the content and payload information will now be described using homomorphic cryptography using the El Gamal method. Figure 4 is a flow chart illustrating the homomorphic cryptography according to this embodiment of the invention. At the trusted server 202, the management processor 203, for example, chooses random numbers r and k1 and g in step 402 and derives g^r and $h_1 = g^{k1}$ in step 404. The encryption device 212 then computes the encrypted content signal c_x where $c_x= h_1^r g^x$ in step 406 and provides the pair (g^r, c_x) to the client. The encryption device 214 then computes in step 408 the encrypted payload information signal c_w where $c_w= h_2(i)^r g^w$ where for each client (i), the server chooses a k2(i) and a k(i)= k1+k2(i) and $h_2(i)=g^{k2(i)}$ where k(i) is known to the client.

After (g^r, c_x) and c_w are transmitted to the client 218 over the network 216, the client 218 combines c_x and c_w in step 410 where $c = c_w \cdot c_x = (h_1^r g^x) \cdot (h_2(i)^r g^w)= h(i)^r \cdot g^{x+w}$, where $h(i)^r=h_1^r \cdot h_2(i)^r$. The client then computes $h(i)^r= (g^r)^{k(i)}$ and decrypts x+w in step 412.

For the decryption the client performs the operation

$$g^{x+w} = \frac{c}{h(i)^r} = \frac{h(i)^r g^{x+w}}{h(i)^r} \qquad (5)$$

where x+w is obtained by inverting the discrete exponential function g^{x+w}. Assuming x+w is of small word length (say in the order of 8 – 16 bits), the inverse is computed via a look up table (LUT).

In another embodiment of the invention according to Fig. 5, a computer readable medium is illustrated schematically. A computer-readable medium 500 has embodied thereon a computer program 510 for embedding a watermark in a media signal in a device, for processing by a computer 513. The computer program 510 comprises a first code segment 514 for providing an at least partially encrypted media signal c_x of said media signal x, wherein encryption is performed using a first encryption key k1; a second code segment 515 for providing an at least partially encrypted watermark signal c_w, wherein encryption is performed using a second encryption key k2; a third code segment 516 for combining the at least partially encrypted media signal c_x and the at least partially encrypted watermark signal c_w in a combiner to obtain an encrypted combined media signal c_y; and a fourth code segment 517 for obtaining a decrypted watermarked media signal y by decrypting said encrypted combined media signal c_y using a third decryption key k3.

The invention can be implemented in any suitable form including hardware, software, firmware or any combination of these. However, preferably, the invention is implemented as computer software running on one or more data processors and/or digital signal processors. The elements and components of an embodiment of the invention may be physically, functionally and logically implemented in any suitable way. Indeed, the functionality may be implemented in a single unit, in a plurality of units or as part of other functional units. As such, the invention may be implemented in a single unit, or may be physically and functionally distributed between different units and processors.

Although the present invention has been described above with reference to specific embodiments, it is not intended to be limited to the specific form set forth herein. Rather, the invention is limited only by the accompanying claims and, other embodiments than the specific above are equally possible within the scope of these appended claims, e.g. different distribution systems than those described above.

In the claims, the term "comprises/comprising" does not exclude the presence of other elements or steps. Furthermore, although individually listed, a plurality of means, elements or method steps may be implemented by e.g. a single unit or processor. Additionally, although individual features may be included in different claims, these may possibly advantageously be combined, and the inclusion in different claims does not imply that a combination of features is not feasible and/or advantageous. In addition, singular references do not exclude a plurality. The terms "a", "an", “first”, “second” etc do not preclude a plurality. Reference signs in the claims are provided merely as a clarifying example and shall not be construed as limiting the scope of the claims in any way.

CLAIMS:

1. A method for embedding a watermark in a media signal x, comprising:

- providing an at least partially encrypted media signal c_x of said media signal x, wherein encryption is performed using a first encryption key k1;
- providing an at least partially encrypted watermark signal c_w, wherein encryption is performed using a second encryption key k2;
- combining the at least partially encrypted media signal c_x and the at least partially encrypted watermark signal c_w in a combiner to obtain an encrypted combined media signal c_y; and
- obtaining a decrypted watermarked media signal y by decrypting said encrypted combined media signal c_y using a third decryption key k3.

2. Method according to claim 1, wherein said combiner is a multiplier.

3. Method according to claim 1, wherein both a first watermark that is comprised in said at least partially encrypted watermark signal c_w and a second watermark of said decrypted watermarked media signal y are identical.

4. Method according to claim 1, wherein said third decryption key k3 differs from said first encryption key k1 and does not decrypt said at least partially encrypted media signal c_x.

5. Method according to claim 1, wherein said third decryption key k3 differs from said second encryption key k2 and does not decrypt said at least partially encrypted watermark signal c_w.

6. Method according to claim 1, wherein said third decryption key k3 differs from said first encryption key k1 and said second encryption key k2.

7. Method according to claim 1 or 2, wherein said at least partially encrypted media signal c_x is encrypted according to the relation:

$$c_x = (1+K)^x r^{k1} \bmod K^2 \text{ or } c_x = (1+K)^x r^{N.k1} \bmod K^2;$$

wherein N, K and r are positive integers and k1 = K-k2 is said first encryption key.

8. Method according to claim 1, 2 or 7, wherein said at least partially encrypted watermark signal c_w is encrypted according to the relation:

$$c_w = (1+K)^w r^{k2} \bmod K^2 \text{ or } c_w = (1+K)^w r^{N.k2} \bmod K^2;$$

wherein N, K and r are positive integers and k2 = K-k1 is said second encryption key.

9. Method according to claim 1, 2, 7 or 8, wherein said obtaining a decrypted watermarked media signal y comprises computing:

$$y = \frac{(c_y{}^N - 1) \bmod k3^2}{Nk3} \bmod k3 \quad \text{or} \quad y = \frac{(c_y - 1) \bmod k3^2}{k3} \bmod k3$$

wherein $c_y = c_x c_w$, N is a positive integer, and k3 = k1+k2 is said third decryption key.

10. Method according to claim 1 or 2, wherein said at least partially encrypted media signal c_x is encrypted according to the relation:

$$c_x = g^{rk1} g^x;$$

wherein g and r are positive integers and k1 is said first encryption key.

11. Method according to claim 1 or 2, wherein said at least partially encrypted watermark signal c_w is encrypted according to the relation: $c_w = g^{rk2} g^w$;

wherein g and r are positive integers and k2 is said second encryption key.

12. Method according to claim 10 or 11, wherein said obtaining a decrypted watermarked media signal y comprises:

computing $g^{x+w} = \dfrac{c_y}{g^{rk3}}$,

wherein $c_y = c_x c_w$, r is a positive integer, and k3=k1+k2 is said third decryption key; and solving the discrete exponential function g^{x+w} using a look up table to obtain the decrypted watermarked media signal y.

13. Method according to claim 1, wherein said method is performed in a device and wherein said device is an untrusted device having an untrusted environment, and/or wherein said providing said at least partially encrypted media signal c_x of said media signal x comprises receiving said at least partially encrypted media signal c_x of said media signal x in said device, and wherein said providing said at least partially encrypted watermark signal c_w comprises receiving said at least partially encrypted watermark signal c_w in said device.

14. The method according to claims 1-13, comprising independently providing said partially encrypted media signal c_x and said partially encrypted watermark signal c_w at independent moments and via independent channels.

15. Method according to any preceding claim, wherein said method is performed in a software or program element and wherein said software or program element is running in an untrusted environment.

16. A system (200) for embedding a watermark in a media signal x, comprising:

- means (219) for providing an at least partially encrypted media signal c_x of said media signal x, wherein encryption is performed using a first encryption key k1;
- means (219) for providing an at least partially encrypted watermark signal c_w, wherein encryption is performed using a second encryption key k2;
- means (220) for combining the at least partially encrypted media signal c_x and the at least partially encrypted watermark signal c_w in a combiner to obtain an encrypted combined media signal c_y; and
- means (222) for obtaining a decrypted watermarked media signal y by decrypting said encrypted combined media signal c_y using a third decryption key k3.

17. A computer-readable medium having embodied thereon a computer program for embedding a watermark in a media signal x, for processing by a computer, the computer program comprising:

- a first code segment for providing an at least partially encrypted media signal c_x of said media signal x, wherein encryption is performed using a first encryption key k1;

- a second code segment for providing an at least partially encrypted watermark signal c_w, wherein encryption is performed using a second encryption key k2;
- a third code segment for combining the at least partially encrypted media signal c_x and the at least partially encrypted watermark signal c_w in a combiner to obtain an encrypted combined media signal c_y; and
- a fourth code segment for obtaining a decrypted watermarked media signal y by decrypting said encrypted combined media signal c_y using a third decryption key k3.

18. An encrypted combined media signal c_y comprising in combination

- an at least partially encrypted media signal c_x of a media signal x, wherein encryption is performed using a first encryption key k1, and
- an at least partially encrypted watermark signal c_w, wherein encryption is performed using a second encryption key k2; wherein

said combination signal is decryptable in order to provide a decrypted watermarked media signal y by decrypting said encrypted combined media signal c_y using a third decryption key k3, such that said watermarked media signal y has a decrypted watermark embedded therein.

19. Use of the method according to claims 1-15 in an electronic music delivery (EMD) system (200).

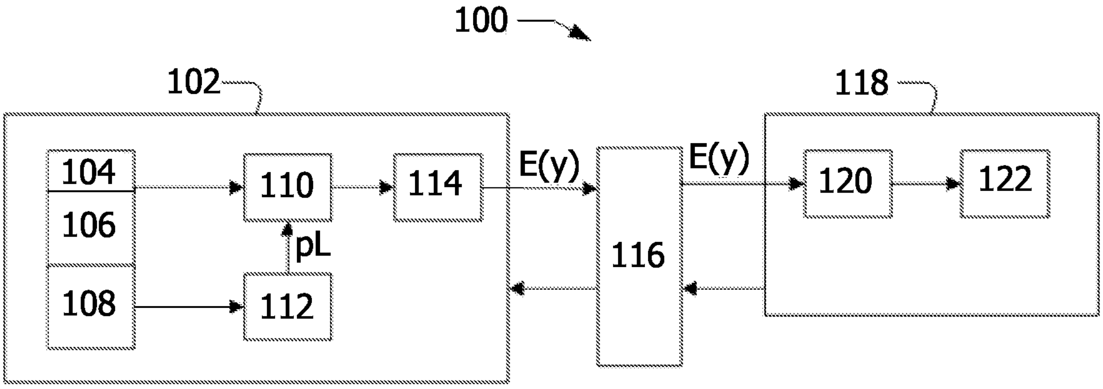

100
102
104
106
108
110
112
pL
114
E(y)
116
E(y)
118
120
122

FIG.1

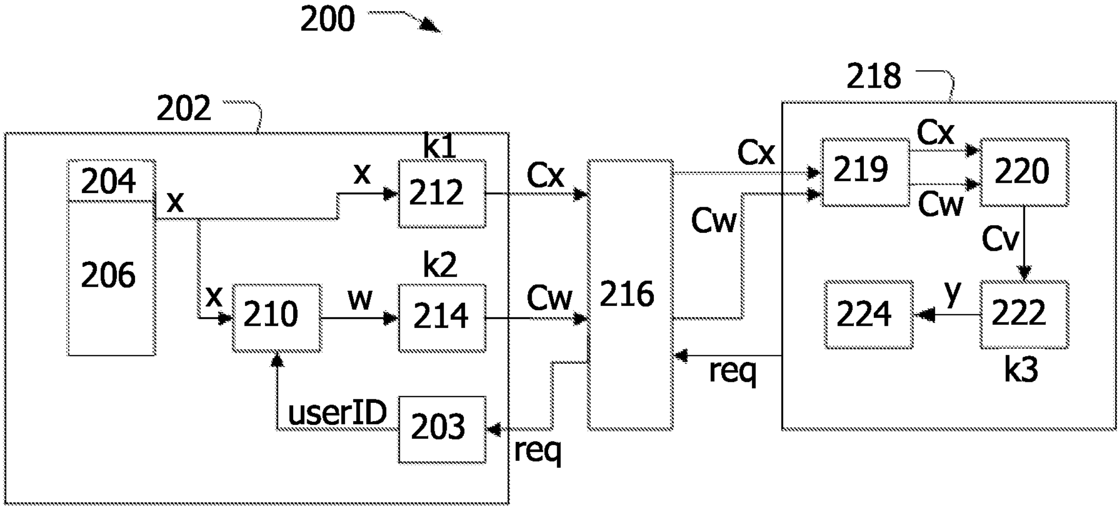

200
202
204
206
x
x
k1
212
x
210
w
k2
214
userID
203
req
Cx
Cw
216
Cx
Cw
req
218
219
Cx
Cw
220
Cv
224
y
222
k3

FIG.2

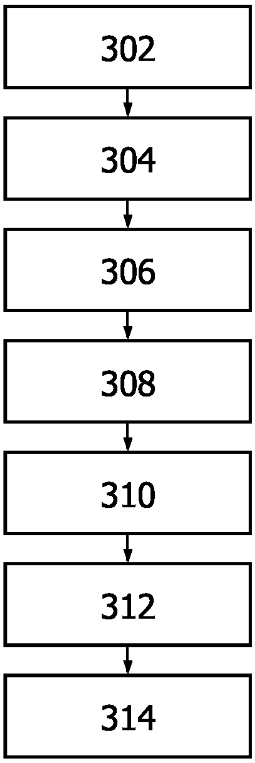


FIG.3

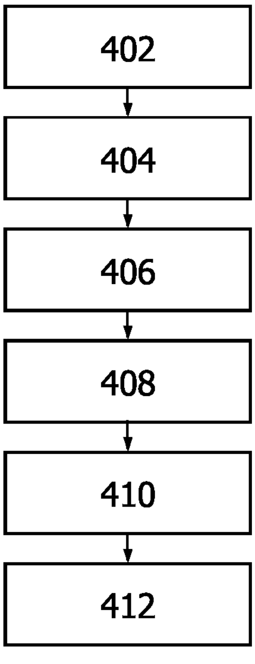


FIG.4

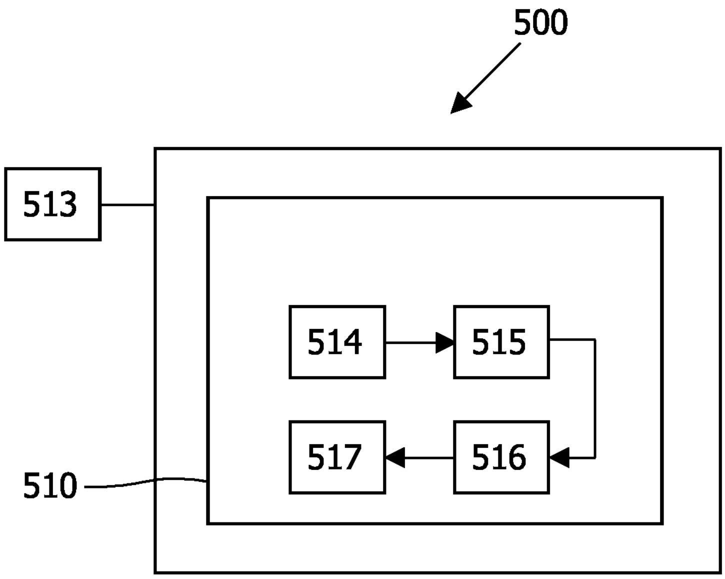


FIG.5

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2006/051773

A. CLASSIFICATION OF SUBJECT MATTER
INV. G10L19/00 G06T1/00 H04N7/26

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)
G10L G06T H04N

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, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	S. KATZENBEISSER: "D.WVL.5 First summary report on hybrid systems" ECRYPT, 31 May 2005 (2005-05-31), XP002401346 Magdeburg, D	1-6, 10-18
Y	pages 11-16	19
Y	VEEN VAN DER M ET AL: "WATERMARKING AND FINGERPRINTING FOR ELECTRONIC MUSIC DELIVERY" PROCEEDINGS OF THE SPIE, SPIE, BELLINGHAM, VA, US, vol. 5306, 2004, pages 200-211, XP008037770 ISSN: 0277-786X abstract	19
	-/--	

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

☒ See patent family 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 2 October 2006	Date of mailing of the international search report 16/10/2006
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 Quélavoine, Régis

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2006/051773

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HAK SOO JU, HYUN JEONG KIM, DONG HOON LEE, JONG IN LIM: "An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control" ICISC 2002, , - 29 November 2002 (2002-11-29) pages 421-432, XP002401347 Seoul, Korea * section 2.1 Memon-Wong's scheme *	1-6, 13-19
P,X	EP 1 612 727 A (CANON RESEARCH CENTRE FRANCE; INRIA INSTITUT NATIONAL DE RECHERCHE EN) 4 January 2006 (2006-01-04) abstract paragraphs [0005], [0040]	1-6, 10-19
P,X	KATZENBEISSER, KALKER: "Structure preserving cryptography" BIRS 05W5505, 23 July 2005 (2005-07-23), - 28 July 2005 (2005-07-28) XP002401348 Calgary, Canada the whole document	1-6, 10-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2006/051773

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1612727 A	04-01-2006	FR 2872373 A1	30-12-2005