РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2007 144 588** (13) **A**

(51) МПК
G10L 19/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2007144588/09, 02.06.2006**

(30) Конвенционный приоритет:
03.06.2005 EP 05104828.8

(43) Дата публикации заявки: **10.06.2009** Бюл. № **16**

(85) Дата перевода заявки PCT на национальную фазу: **30.11.2007**

(86) Заявка PCT:
IB 2006/051773 (02.06.2006)

(87) Публикация PCT:
WO 2006/129293 (07.12.2006)

Адрес для переписки:
129090, Москва, ул.Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. А.В.Мицу, рег.№ 364

(71) Заявитель(и):
КОНИНКЛЕЙКЕ ФИЛИПС ЭЛЕКТРОНИКС Н.В. (NL)

(72) Автор(ы):
ЛЕММА Авеке Н. (NL),
ВАН ДЕР ВЕН Минне (NL),
ТЮЙЛС Пим Т. (NL),
КАЛКЕР Антониус А. К. М. (NL)

(54) ГОМОМОРФНОЕ ШИФРОВАНИЕ ДЛЯ ЗАЩИТЫ ВОДЯНОГО ЗНАКА

(57) Формула изобретения

1. Способ вставки водяного знака в медиасигнал x, содержащий этапы, на которых:

обеспечивают по меньшей мере частично зашифрованный медиасигнал c_x упомянутого медиасигнала x, при этом шифрование выполняется с использованием первого ключа k1 шифрования;

обеспечивают по меньшей мере частично зашифрованный сигнал c_w с водяным знаком, при этом шифрование выполняется с использованием второго ключа k2 шифрования;

объединяют по меньшей мере частично зашифрованный медиасигнал c_x и по меньшей мере частично зашифрованный сигнал c_w с водяным знаком в блоке объединения для получения зашифрованного объединенного медиасигнала c_y и

получают дешифрованный медиасигнал y, помеченный водяным знаком, посредством дешифрования упомянутого объединенного медиасигнала c_y с помощью третьего ключа k3 дешифрования.

2. Способ по п.1, в котором упомянутый блок объединения является умножителем.

3. Способ по п.1, в котором первый водяной знак, который содержится в упомянутом по меньшей мере частично зашифрованном сигнале c_w с водяным знаком, и второй водяной знак упомянутого дешифрованного медиасигнала y, помеченного

RU 2007144588 A

RU 2007144588 A

водяным знаком, являются идентичными.

4. Способ по п.1, в котором упомянутый третий ключ k3 дешифрования отличается от упомянутого первого ключа k1 шифрования и не дешифрует упомянутый по меньшей мере частично зашифрованный медиасигнал c_x.

5. Способ по п.1, в котором упомянутый третий ключ k3 дешифрования отличается от упомянутого второго ключа k2 шифрования и не дешифрует упомянутый по меньшей мере частично зашифрованный сигнал c_w с водяным знаком.

6. Способ по п.1, в котором упомянутый третий ключ дешифрования k3 отличается от упомянутого первого ключа k1 шифрования и упомянутого второго ключа k2 шифрования.

7. Способ по п.1, в котором упомянутый по меньшей мере частично зашифрованный медиасигнал c_x шифруется в соответствии с формулой

$c_x=(1+K)^x r^{k1} \mathrm{mod} K^2$ или $c_x=(1+K)^x r^{N,k1} \mathrm{mod} K^2$,

где N, K и r являются положительными целыми числами и k1=K-k2 является упомянутым первым ключом шифрования.

8. Способ по п.1, в котором упомянутый по меньшей мере частично зашифрованный сигнал c_w с водяным знаком шифруется в соответствии с формулой

$c_w=(1+K)^w r^{k2} \mathrm{mod} K^2$ или $c_w=(1+K)^w r^{N,k2} \mathrm{mod} K^2$,

где N, K и r являются положительными целыми числами и k2=K-k1 является упомянутым вторым ключом шифрования.

9. Способ по п.1, в котором упомянутое получение дешифрованного медиасигнала y, помеченного водяным знаком, содержит вычисление

$$y=\frac{(c_y^N-1)\mathrm{mod} k3^2}{Nk3}\mathrm{mod} k3 \quad \text{или} \quad y=\frac{(c_y-1)\mathrm{mod} k3^2}{k3}\mathrm{mod} k3,$$

где $c_y=c_x c_w$, N является положительным целым числом и k3=k1+k2 является третьим ключом дешифрования.

10. Способ по п.1, в котором упомянутый по меньшей мере частично зашифрованный медиасигнал c_x шифруется в соответствии с формулой

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

где g и r являются положительными целыми числами и k1 является упомянутым первым ключом шифрования.

11. Способ по п.1, в котором упомянутый по меньшей мере частично зашифрованный сигнал c_w с водяным знаком шифруется в соответствии с формулой

$c_w=g^{rk2} g^w$,

где g и r являются положительными целыми числами и k2 является упомянутым вторым ключом шифрования.

12. Способ по п.10 или 11, в котором упомянутое получение дешифрованного медиасигнала y, помеченного водяным знаком, содержит вычисление,

где $c_y=c_x c_w$, r является положительным целым числом и k3=k1+k2 является упомянутым третьим ключом дешифрования; и

решение дискретной экспоненциальной функции g^{x+w}, используя справочную таблицу, для получения дешифрованного медиасигнала y, помеченного водяным знаком.

13. Способ по п.1, в котором упомянутый способ выполняется в устройстве и при этом упомянутое устройство является ненадежным устройством, имеющим ненадежную среду, и/или при этом упомянутое обеспечение упомянутого по меньшей

RU 2007144588 A

RU 2007144588 A

мере частично зашифрованного медиасигнала c_x упомянутого медиасигнала x содержит прием упомянутого по меньшей мере частично зашифрованного медиасигнала c_x упомянутого медиасигнала x в упомянутом устройстве и при этом упомянутое обеспечение упомянутого по меньшей мере частично зашифрованного сигнала c_w с водяным знаком содержит прием упомянутого по меньшей мере частично зашифрованного сигнала c_w с водяным знаком в упомянутом устройстве.

14. Способ по п.1, содержащий независимое обеспечение упомянутого частичного зашифрованного медиасигнала c_x и упомянутого по меньшей мере частично зашифрованного сигнала c_w с водяным знаком в независимые моменты и по независимым каналам.

15. Способ по п.1, причем упомянутый способ выполняется на программном обеспечении или программном элементе и в котором упомянутое программное обеспечение или программный элемент выполняется в ненадежной среде.

16. Система (200) для вставки водяного знака в медиасигнал x, содержащая:

средство (219) для обеспечения по меньшей мере частично зашифрованного медиасигнала c_x упомянутого медиасигнала x, при этом шифрование выполняется с использованием первого ключа k1 шифрования;

средство (219) для обеспечения по меньшей мере частично зашифрованного сигнала c_w с водяным знаком, при этом шифрование выполняется с использованием второго ключа шифрования k2;

средство (220) для объединения по меньшей мере частично зашифрованного медиасигнала c_x и по меньшей мере частично зашифрованного сигнала c_w с водяным знаком в блоке объединения для получения объединенного зашифрованного медиасигнала c_y;

средство (222) для получения дешифрованного медиасигнала y, помеченного водяным знаком, посредством дешифрования упомянутого объединенного зашифрованного медиасигнала c_y с использованием третьего ключа k3 дешифрования.

17. Машиночитаемый носитель, имеющий воплощенную на нем компьютерную программу для вставки водяного знака в медиасигнал x, для обработки компьютером, компьютерная программа содержит:

первый кодовый сегмент для обеспечения по меньшей мере частично зашифрованного медиасигнала c_x упомянутого медиасигнала x, при этом шифрование выполняется с использованием первого ключа k1 шифрования;

второй кодовый сегмент для обеспечения по меньшей мере частично зашифрованного сигнала c_w с водяным знаком, при этом шифование выполняется с использованием второго ключа k2 шифрования;

третий кодовый сегмент для объединения по меньшей мере частично зашифрованного медиасигнала c_x и по меньшей мере частично зашифрованного сигнала c_w с водяным знаком в блоке объединения для получения зашифрованного объединенного медиасигнала c_y; и

четвертый кодовый сегмент для получения дешифрованного медиасигнала y, помеченного водяным знаком, посредством дешифрования упомянутого шифрованного объединенного медиасигнала c_y с использованием третьего ключа k3 дешифрования.

18. Зашифрованный объединенный медиасигнал c_y, содержащий в комбинации по меньшей мере частично зашифрованный медиасигнал c_x медиасигнала x, при

RU 2007144588 A

RU 2007144588 A

этом шифрование выполняется с использованием первого ключа k1 шифрования; и

по меньшей мере частично зашифрованный сигнал c_w с водяным знаком, при этом упомянутое шифрование выполняется с использованием второго ключа k2 шифрования; при этом

упомянутый объединенный сигнал дешифруется для получения дешифрованного медиасигнала y, помеченного водяным знаком, посредством дешифрования упомянутого объединенного медиасигнала c_y с использованием третьего ключа k3 дешифрования таким образом, что упомянутый медиасигнал y, помеченный водяным знаком, имеет дешифрованный водяной знак, вставленный в него.

19. Использование способа по любому из пп.1-15 в системе (200) доставки электронной музыки (EMD).

RU 2007144588 A

RU 2007144588 A