【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成21年7月16日(2009.7.16)

【公表番号】特表2008-546019(P2008-546019A)
【公表日】平成20年12月18日(2008.12.18)
【年通号数】公開・登録公報2008-050
【出願番号】特願2008-514292(P2008-514292)
【国際特許分類】
Ｇ０９Ｃ　5/00　(2006.01)
Ｈ０４Ｎ　1/387　(2006.01)
Ｇ０６Ｔ　1/00　(2006.01)
Ｇ１０Ｌ　19/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　5/00
Ｈ０４Ｎ　1/387
Ｇ０６Ｔ　1/00　５００Ｂ
Ｇ１０Ｌ　19/00　２３０

【手続補正書】
【提出日】平成21年6月1日(2009.6.1)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
メディア信号xにウォーターマークを埋め込む方法において、
暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号xの少なくとも部分的に暗号化されたメディア信号c_xを提供するステップと、
暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号c_wを提供するステップと、
暗号化された結合メディア信号c_yを得るように結合器において前記少なくとも部分的に暗号化されたメディア信号c_x及び前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを結合するステップと、
第３の復号鍵k3を使用して前記暗号化された結合メディア信号c_yを復号することにより復号されたウォーターマーク入りメディア信号yを得るステップと、
を有する方法。
【請求項２】
前記結合器が乗算器である、請求項１に記載の方法。
【請求項３】
前記少なくとも部分的に暗号化されたウォーターマーク信号c_wに含まれる第１のウォーターマーク及び前記復号されたウォーターマーク入りメディア信号yの第２のウォーターマークの両方が同一である、請求項１に記載の方法。
【請求項４】
前記第３の復号鍵k3が、前記第１の暗号化鍵k1とは異なり、前記少なくとも部分的に暗号化されたメディア信号c_xを復号しない、請求項１に記載の方法。
【請求項５】
前記第３の復号鍵k3が、前記第２の暗号化鍵k2とは異なり、前記少なくとも部分的に暗

号化されたウォーターマーク信号c_wを復号しない、請求項１に記載の方法。
【請求項６】
前記第３の復号鍵k3が、前記第１の暗号化鍵k1及び前記第２の暗号化鍵k2とは異なる、請求項１に記載の方法。
【請求項７】
前記少なくとも部分的に暗号化されたメディア信号c_xが、
$c_x = (1+K)^x r^{k1} \bmod K^2$ 又は $c_x = (1+K)^x r^{N \cdot k1} \bmod K^2$
の関係によって暗号化され、ここでN、K及びrが正の整数であり、k1 = K-k2が前記第１の暗号化鍵である、請求項１又は２に記載の方法。
【請求項８】
前記少なくとも部分的に暗号化されたウォーターマーク信号c_wが、
$c_w = (1+K)^w r^{k2} \bmod K^2$ 又は $c_w = (1+K)^w r^{N \cdot k2} \bmod K^2$
の関係によって暗号化され、ここでN、K及びrが正の整数であり、k2 = K-k1が前記第２の暗号化鍵である、請求項１、２又は７に記載の方法。
【請求項９】
前記復号されたウォーターマーク入りメディア信号yを得るステップが、
$y = ((c_y^N - 1) \bmod k3^2)/Nk3 \bmod k3$ 又は $y = ((c_y - 1) \bmod k3^2)/k3 \bmod k3$
を計算し、ここで$c_y = c_x c_w$であり、Nが正の整数であり、k3 = k1+k2が前記第３の復号鍵である、請求項１、２、７又は８に記載の方法。
【請求項１０】
前記少なくとも部分的に暗号化されたメディア信号c_xが、
$c_x = g^{rk1} g^x$
の関係によって暗号化され、ここでg及びrが正の整数であり、k1が前記第１の暗号化鍵である、請求項１又は２に記載の方法。
【請求項１１】
前記少なくとも部分的に暗号化されたウォーターマーク信号c_wが、$c_w = g^{rk2} g^w$の関係によって暗号化され、ここでg及びrが正の整数であり、k2が前記第２の暗号化鍵である、請求項１又は２に記載の方法。
【請求項１２】
前記復号されたウォーターマーク入りメディア信号yを得るステップが、
$g^{x+w} = c_y / g^{rk3}$を計算するステップであって、$c_y = c_x c_w$であり、rが正の整数であり、k3 = k1+k2が前記第３の復号鍵である、当該計算するステップと、
前記復号されたウォーターマーク入りメディア信号yを得るためにルックアップテーブルを使用して離散的な指数関数g^{x+w}を解くステップと、
を有する、請求項１０又は１１に記載の方法。
【請求項１３】
前記方法がデバイスにおいて実行され、前記デバイスが、信用されていない環境を持つ信用されていないデバイスであり、及び／又は前記メディア信号xの少なくとも部分的に暗号化されたメディア信号c_xを提供するステップが、前記デバイスにおいて前記メディア信号xの前記少なくとも部分的に暗号化されたメディア信号c_xを受信するステップを有し、前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを提供するステップが、前記デバイスにおいて前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを受信するステップを有する、請求項１に記載の方法。
【請求項１４】
独立した瞬間において及び独立したチャネルを介して前記少なくとも部分的に暗号化されたメディア信号c_x及び前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを独立して提供するステップを有する、請求項１ないし１３のいずれか一項に記載の方法。
【請求項１５】
前記方法が、ソフトウェア又はプログラム要素において実行され、前記ソフトウェア又はプログラム要素が、信用されていない環境で実行される、請求項１ないし１４のいずれ

か一項に記載の方法。
【請求項１６】
メディア信号xにウォーターマークを埋め込むシステムにおいて、
暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号xの少なくとも部分的に暗号化されたメディア信号c_xを提供する手段と、
暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号c_wを提供する手段と、
暗号化された結合メディア信号c_yを得るように結合器において前記少なくとも部分的に暗号化されたメディア信号c_x及び前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを結合する手段と、
第３の復号鍵k3を使用して前記暗号化された結合メディア信号c_yを復号することにより復号されたウォーターマーク入りメディア信号yを得る手段と、
を有するシステム。
【請求項１７】
コンピュータにより処理する、メディア信号xにウォーターマークを埋め込むコンピュータプログラムを包含するコンピュータ読み取り可能媒体において、前記コンピュータプログラムが、
暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号xの少なくとも部分的に暗号化されたメディア信号c_xを提供する第１のコードセグメントと、
暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号c_wを提供する第２のコードセグメントと、
暗号化された結合メディア信号c_yを得るように結合器において前記少なくとも部分的に暗号化されたメディア信号c_x及び前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを結合する第３のコードセグメントと、
第３の復号鍵k3を使用して前記暗号化された結合メディア信号c_yを復号することにより復号されたウォーターマーク入りメディア信号yを得る第４のコードセグメントと、
を有する、コンピュータ読み取り可能媒体。
【請求項１８】
電子音楽配信（ＥＭＤ）システムにおける請求項１ないし１５のいずれか一項に記載の方法の使用。