【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３区分
【発行日】平成20年1月24日(2008.1.24)

【公開番号】特開2007-317175(P2007-317175A)
【公開日】平成19年12月6日(2007.12.6)
【年通号数】公開・登録公報2007-047
【出願番号】特願2007-118387(P2007-118387)
【国際特許分類】
Ｇ０６Ｆ　21/24　(2006.01)
Ｇ０９Ｃ　5/00　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｇ０６Ｆ　21/00　(2006.01)
Ｈ０４Ｎ　7/16　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　５６０Ｂ
Ｇ０９Ｃ　5/00
Ｇ０９Ｃ　1/00　６４０Ｄ
Ｇ０６Ｆ　12/14　５５０Ｂ
Ｇ０６Ｆ　12/14　５６０Ｃ
Ｇ０６Ｆ　15/00　３３０Ｚ
Ｈ０４Ｎ　7/16　Ｚ

【手続補正書】
【提出日】平成19年11月6日(2007.11.6)
【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】
コンテンツを受信装置へ送信する送信装置であって、
１個のコンテンツからその全部又は一部を抽出して追跡情報を生成し、生成した追跡情報を複数個複製する複製手段と、
複数個の追跡情報のそれぞれに対応した複数個の候補情報を取得する候補情報取得手段と、
前記複数個の候補情報のうちから受信装置により選択された１個の候補情報に依存して生成された証拠情報を取得する証拠情報取得手段と、
前記複数個の候補情報のそれぞれに基づいて、複数個のハッシュ値を生成するハッシュ生成手段と、
各追跡情報に、当該追跡情報に対応する候補情報に基づいて生成された前記ハッシュ値を埋め込み、各追跡情報に、前記証拠情報を埋め込む埋込手段と、
ハッシュ値と証拠情報とが埋め込まれた各追跡情報を送信する送信手段と
を備えることを特徴とする送信装置。
【請求項２】
前記コンテンツは、動画及び／又は音声から構成されるマルチメディアデータであり、
前記埋込手段は、前記追跡情報に対して、電子透かし技術を用いて、前記ハッシュ値及び前記証拠情報を埋め込む
ことを特徴とする請求項１に記載の送信装置。

【請求項３】
前記送信装置は、さらに、
前記追跡情報を秘匿通信処理するために用いる複数個のコンテンツ鍵データを生成するコンテンツ鍵生成手段を備え、
前記複数個の候補情報のそれぞれは、前記コンテンツ鍵データのそれぞれに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項４】
前記送信装置は、さらに、
前記追跡情報を暗号処理するために用いる複数個のコンテンツ鍵データと、前記複数個のコンテンツ鍵データのそれぞれを識別する複数個のコンテンツ鍵データ識別子とを生成するコンテンツ鍵生成手段を備え、
前記複数個の候補情報のそれぞれは、前記コンテンツ鍵データ識別子のそれぞれに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項５】
前記送信装置は、さらに、
当該送信装置に対応付けられている公開鍵データと秘密鍵データとを保持しており、
前記複数個の候補情報のそれぞれは、前記公開鍵データに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項６】
前記送信装置は、さらに、
前記追跡情報を秘匿通信処理するために用いる複数個の乱数データを生成する乱数生成手段を備え、
前記複数個の候補情報のそれぞれは、前記乱数データのそれぞれに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項７】
前記送信装置は、さらに、
当該送信装置に対応付けられている複数個の公開鍵データ及び秘密鍵データを保持しており、
前記複数個の候補情報のそれぞれは、前記複数個の公開鍵データに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項８】
前記送信装置は、さらに、
当該送信装置に対応付けられている複数個の公開鍵データ、秘密鍵データ、及び公開鍵識別子を保持しており、
前記複数個の候補情報のそれぞれは、前記複数個の公開鍵識別子に基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項９】
前記証拠情報は、前記受信装置に対応付けられている公開鍵暗号の公開鍵データに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項１０】
前記証拠情報は、前記受信装置に対応付けられている公開鍵暗号の秘密鍵データに基づき生成された電子署名データを含む
ことを特徴とする請求項２に記載の送信装置。
【請求項１１】
送信装置からコンテンツを受信する受信装置であって、
１個のコンテンツの全部又は一部が複製されて生成された複数個の追跡情報のそれぞれに対応する複数個の候補情報のうちから、１個の候補情報を選択する選択手段と、

選択した前記候補情報に基づき、証拠情報を生成する生成手段と、
前記証拠情報を前記送信装置へ送信する送信手段と、
前記送信装置から、選択した前記候補情報に対応する追跡情報を取得する取得手段と
を備えることを特徴とする受信装置。
【請求項１２】
送信装置から受信装置へコンテンツを転送するコンテンツ配信システムであって、
前記送信装置は、
１個のコンテンツからその全部又は一部を抽出して追跡情報を生成し、生成した追跡情報を複数個複製する複製手段と、
複数個の追跡情報のそれぞれに対応した複数個の候補情報を取得する候補情報取得手段と、
前記複数個の候補情報のうちから受信装置により選択された１個の候補情報に依存して生成された証拠情報を取得する証拠情報取得手段と、
前記複数個の候補情報のそれぞれに基づいて、複数個のハッシュ値を生成するハッシュ生成手段と、
各追跡情報に、当該追跡情報に対応する候補情報に基づいて生成された前記ハッシュ値を埋め込み、各追跡情報に、前記証拠情報を埋め込む埋込手段と、
ハッシュ値と証拠情報とが埋め込まれた各追跡情報を送信する送信手段とを備え、
前記受信装置は、
前記複数個の追跡情報のそれぞれに対応する複数個の候補情報のうちから、１個の候補情報を選択する選択手段と、
選択した前記候補情報に基づき、証拠情報を生成する生成手段と、
前記証拠情報を前記送信装置へ送信する送信手段と、
前記送信装置から、選択した前記候補情報に対応する追跡情報を取得する取得手段とを備える
ことを特徴とするコンテンツ配信システム。
【請求項１３】
コンテンツを受信装置へ送信する送信装置で用いられるコンテンツ送信方法であって、
１個のコンテンツからその全部又は一部を抽出して追跡情報を生成し、生成した追跡情報を複数個複製する複製ステップと、
複数個の追跡情報のそれぞれに対応した複数個の候補情報を取得する候補情報取得ステップと、
前記複数個の候補情報のうちから受信装置により選択された１個の候補情報に依存して生成された証拠情報を取得する証拠情報取得ステップと、
前記複数個の候補情報のそれぞれに基づいて、複数個のハッシュ値を生成するハッシュ生成ステップと、
各追跡情報に、当該追跡情報に対応する候補情報に基づいて生成された前記ハッシュ値を埋め込み、各追跡情報に、前記証拠情報を埋め込む埋込ステップと、
ハッシュ値と証拠情報とが埋め込まれた各追跡情報を送信する送信ステップと
を含むことを特徴とするコンテンツ送信方法。
【請求項１４】
コンテンツを受信装置へ送信する送信装置で用いられるコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、
前記コンピュータプログラムは、
１個のコンテンツからその全部又は一部を抽出して追跡情報を生成し、生成した追跡情報を複数個複製する複製ステップと、
複数個の追跡情報のそれぞれに対応した複数個の候補情報を取得する候補情報取得ステップと、
前記複数個の候補情報のうちから受信装置により選択された１個の候補情報に依存して生成された証拠情報を取得する証拠情報取得ステップと、

前記複数個の候補情報のそれぞれに基づいて、複数個のハッシュ値を生成するハッシュ生成ステップと、
各追跡情報に、当該追跡情報に対応する候補情報に基づいて生成された前記ハッシュ値を埋め込み、各追跡情報に、前記証拠情報を埋め込む埋込ステップと、
ハッシュ値と証拠情報とが埋め込まれた各追跡情報を送信する送信ステップと
を含むことを特徴とする記録媒体。
【請求項１５】
コンテンツを受信装置へ送信する送信装置で用いられる集積回路であって、
１個のコンテンツからその全部又は一部を抽出して追跡情報を生成し、生成した追跡情報を複数個複製する複製手段と、
複数個の追跡情報のそれぞれに対応した複数個の候補情報を取得する候補情報取得手段と、
前記複数個の候補情報のうちから受信装置により選択された１個の候補情報に依存して生成された証拠情報を取得する証拠情報取得手段と、
前記複数個の候補情報のそれぞれに基づいて、複数個のハッシュ値を生成するハッシュ生成手段と、
各追跡情報に、当該追跡情報に対応する候補情報に基づいて生成された前記ハッシュ値を埋め込み、各追跡情報に、前記証拠情報を埋め込む埋込手段と、
ハッシュ値と証拠情報とが埋め込まれた各追跡情報を送信する送信手段と
を備えることを特徴とする集積回路。
【請求項１６】
送信装置からコンテンツを受信する受信装置で用いられるコンテンツ受信方法であって、
１個のコンテンツの全部又は一部が複製されて生成された複数個の追跡情報のそれぞれに対応する複数個の候補情報のうちから、１個の候補情報を選択する選択ステップと、
選択した前記候補情報に基づき、証拠情報を生成する生成ステップと、
前記証拠情報を前記送信装置へ送信する送信ステップと、
前記送信装置から、選択した前記候補情報に対応する追跡情報を取得する取得ステップと
を含むことを特徴とするコンテンツ受信方法。
【請求項１７】
送信装置からコンテンツを受信する受信装置で用いられるコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、
前記コンピュータプログラムは、
１個のコンテンツの全部又は一部が複製されて生成された複数個の追跡情報のそれぞれに対応する複数個の候補情報のうちから、１個の候補情報を選択する選択ステップと、
選択した前記候補情報に基づき、証拠情報を生成する生成ステップと、
前記証拠情報を前記送信装置へ送信する送信ステップと、
前記送信装置から、選択した前記候補情報に対応する追跡情報を取得する取得ステップと
を含むことを特徴とする記録媒体。
【請求項１８】
送信装置からコンテンツを受信する受信装置で用いられる集積回路であって、
１個のコンテンツの全部又は一部が複製されて生成された複数個の追跡情報のそれぞれに対応する複数個の候補情報のうちから、１個の候補情報を選択する選択手段と、
選択した前記候補情報に基づき、証拠情報を生成する生成手段と、
前記証拠情報を前記送信装置へ送信する送信手段と、
前記送信装置から、選択した前記候補情報に対応する追跡情報を取得する取得手段と
を備えることを特徴とする集積回路。