

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4174191号

(P4174191)

(45) 発行日 平成20年10月29日 (2008.10.29)

(24) 登録日 平成20年8月22日 (2008.8.22)

(51) Int.Cl. F I
 H O 4 L 9/08 (2006.01) H O 4 L 9/00 6 O 1 B
 H O 4 L 9/32 (2006.01) H O 4 L 9/00 6 7 5 A

請求項の数 5 (全 16 頁)

(21) 出願番号	特願2001-121061 (P2001-121061)	(73) 特許権者	000004237
(22) 出願日	平成13年4月19日 (2001.4.19)		日本電気株式会社
(65) 公開番号	特開2002-319934 (P2002-319934A)		東京都港区芝五丁目7番1号
(43) 公開日	平成14年10月31日 (2002.10.31)	(74) 代理人	100109313
審査請求日	平成14年3月19日 (2002.3.19)		弁理士 机 昌彦
審判番号	不服2005-183 (P2005-183/J1)	(74) 代理人	100121290
審判請求日	平成17年1月5日 (2005.1.5)		弁理士 木村 明隆
		(74) 代理人	100111637
			弁理士 谷澤 靖久
		(72) 発明者	森下 卓也
			東京都港区芝五丁目7番1号 日本電気株
			式会社内
		(72) 発明者	宮内 宏
			東京都港区芝五丁目7番1号 日本電気株
			式会社内

最終頁に続く

(54) 【発明の名称】 著作権保護システム及びその方法

(57) 【特許請求の範囲】

【請求項1】

著作物に係る入力データを暗号化し、出力先の処理装置に対して認証を行って出力することによって該著作物の著作権を保護する著作権保護システムであって、

放送受信装置から出力された暗号化された入力データを暗号解除後入力し、第1の暗号鍵を使用して暗号化し前記処理装置の第1の暗号解除手段に出力する第1の暗号化手段と

前記第1の暗号鍵を生成して前記第1の暗号化手段に提供し、認証鍵に基づいた前記処理装置の第1の認証手段との相互認証の完了を条件として前記認証鍵を使用して前記第1の暗号鍵を暗号化し前記処理装置の第1の認証手段に出力し、暗号に係る鍵の無効情報を有し、前記第1の暗号化手段と前記第1の暗号解除手段の間で前記第1の暗号鍵を共有する際の前記認証に使用する認証鍵の情報が前記無効情報の中に含まれる場合に、前記認証を不可とする第2の認証手段と、

前記放送受信装置から出力された暗号解除前の入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する無効情報更新手段とを具備し、

前記放送受信装置は、暗号解除前の入力データに付随して提供される更新用認証鍵を受け取ると、前記認証鍵を更新する前記処理装置の認証鍵更新手段に前記更新用認証鍵を出力することを特徴とする著作権保護システム。

【請求項2】

前記暗号化の解除に係る機能を実現するための処理プログラムを実行する処理装置を備え、

前記処理装置は、前記入力データに付随して提供される更新用プログラムを受け取ると、前記処理プログラムを更新することを特徴とする請求項 1 に記載の著作権保護システム。

【請求項 3】

著作物に係る入力データを暗号化し、出力先の処理装置に対して認証を行って出力することによって該著作物の著作権を保護する著作権保護システムにおける著作権保護方法であって、

第 1 の暗号鍵を生成する過程と、

放送受信装置から出力された暗号化された入力データを暗号解除後入力し、前記第 1 の暗号鍵を使用して暗号化し前記処理装置の第 1 の暗号解除手段に出力する第 1 の暗号化過程と、

前記第 1 の暗号化を行う手段と前記処理装置の第 1 の暗号解除手段の間で前記第 1 の暗号鍵を共有する際に、認証鍵に基づいた前記処理装置の認証手段との相互認証を行う過程と、

この前記認証に使用する認証鍵の情報が暗号に係る鍵の無効情報の中に含まれる場合に、前記認証を不可とする過程と、

前記認証の完了を条件として、前記認証鍵を使用して前記第 1 の暗号鍵を暗号化し前記処理装置の認証手段に出力する過程と、

前記放送受信装置から出力された暗号化された入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する過程と、

前記放送受信装置から出力された暗号化された入力データに付随して提供される更新用認証鍵を受け取ると、前記認証鍵を更新する過程と、を含むことを特徴とする著作権保護方法。

【請求項 4】

前記入力データに付随して提供される更新用プログラムを受け取る過程と、

この更新用プログラムにより、前記暗号化の解除に係る機能を実現するための処理プログラムを更新する過程と、をさらに含むことを特徴とする請求項 3 に記載の著作権保護方法。

【請求項 5】

著作物に係る入力データを暗号化し、出力先の処理装置に対して認証を行って出力することによって該著作物の著作権を保護する著作権保護システムにおける著作権保護処理を行うための著作権保護プログラムであって、

第 1 の暗号鍵を生成する処理と、

放送受信装置から出力された暗号化された入力データを暗号解除後入力し、前記第 1 の暗号鍵を使用して暗号化し前記処理装置の第 1 の暗号解除手段に出力する第 1 の暗号化処理と、

前記第 1 の暗号化処理を行う手段と前記処理装置の第 1 の暗号解除手段の間で前記第 1 の暗号鍵を共有する際に、認証鍵に基づいた前記処理装置の認証手段との相互認証を行う処理と、

この認証に使用する認証鍵の情報が暗号に係る鍵の無効情報の中に含まれる場合に、前記認証を不可とする処理と、

前記認証の完了を条件として、前記認証鍵を使用して前記第 1 の暗号鍵を暗号化し前記処理装置の認証手段に出力する処理と、

前記放送受信装置から出力された暗号化された入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する処理と、

前記放送受信装置から出力された暗号化された入力データに付随して提供される更新用認証鍵を受け取ると、前記認証鍵を更新する処理と、をコンピュータに実行させることを特徴とする著作権保護プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、放送等により提供される著作物の著作権を暗号化により保護する著作権保護システム及びその方法に関する。

【0002】

【従来の技術】

図3は、従来の著作権保護システムの構成例を示すブロック図である。この図3に示す著作権保護システムは、DVD（Digital Versatile Disc）に記録された著作物の著作権を保護するためのものである。一般に、著作物をDVDに記録して販売する際には、悪意を持った第三者により著作物が不正に使用されることを防止するために、画像や音声など著作物のデータは暗号化された後、DVDに記録される。また、その記録データの暗号解除に必要なディスク鍵とタイトル鍵も暗号化されてDVDに記録される。

10

【0003】

図3の従来の著作権保護システムは、DVD読出し装置21、バス22、バス認証部23、マスター鍵24、ディスク鍵復号部25、タイトル鍵復号部26、デスクランブル部27、及びMP EGデコーダ28を備える。DVD読出し装置21とバス認証部23とデスクランブル部27はそれぞれバス22に接続されており、このバス22を介してデータ伝送が可能である。バス認証部23とデスクランブル部27は、DVD読出し装置21によってDVDから読み出されたデータをバス22を介して取得する。

20

【0004】

次に、上記図3に示す従来の著作権保護システムの動作を説明する。

まず、バス認証部23はバス22を介してDVD読出し装置21との間で相互認証を行い、バス22を介して鍵を伝送するための時変鍵を共有する。次いで、バス認証部23は、DVD読出し装置21によりDVDから暗号化されたディスク鍵とタイトル鍵を読み出して取得し、そのディスク鍵をディスク鍵復号部25へ提供し、またタイトル鍵をタイトル鍵復号部26へ提供する。ディスク鍵復号部25はマスター鍵24によりディスク鍵の暗号を解除してディスク鍵を復号する。タイトル鍵復号部26はディスク鍵復号部25から復号されたディスク鍵を取得し、このディスク鍵によりタイトル鍵の暗号を解除してタイトル鍵を復号し、このタイトル鍵をデスクランブル部27へ提供する。

30

【0005】

次いで、デスクランブル部27は、DVD読出し装置21によりDVDから暗号化された著作物のデータの暗号をタイトル鍵により解除してMP EGデコーダ28へ出力する。MP EGデコーダ28は、その暗号が解除されたデータを使用して画像または音声を再生する。

【0006】

上述したように従来の著作権保護システムにおいては、DVDに記録されているディスク鍵とタイトル鍵の暗号解除に必要なマスター鍵を備え、このマスター鍵なしではディスク鍵とタイトル鍵を復号してDVDに記録されている著作物のデータの暗号を解除することができないようにしている。また、バス22上で伝送されるデータは暗号化されたもので、バス22からデータを取得してもそのデータから再生可能な著作物のデータを取得することは困難である。

40

このようにして従来の著作権保護システムは、悪意を持った第三者により著作物が不正に使用されることを防止するものである。

【0007】

また、上記図3の著作権保護システムは、プログラムを実行可能な処理装置を備えるようにし、この処理装置が各部23及び25～28のそれぞれの機能を実現するためのプログラムを実行して各部23及び25～28を実現することも可能である。これにより、パーソナルコンピュータ等の情報処理装置に図3の著作権保護システムを備えることが可能となっている。

50

【0008】

【発明が解決しようとする課題】

しかし、上述した従来の著作権保護システムでは、悪意を持った第三者によってプログラムの解析などにより認証方式や暗号化方式が解読された場合には、既に利用されている複数の著作権保護システムの暗号に係る鍵（マスター鍵）やプログラムを変更することは困難であり、著作物の不正使用を防止することができないという問題がある。

【0009】

このため、認証方式や暗号化方式などが解読されて著作物が不正に使用された場合に、著作権保護システムの暗号に係る鍵を無効化して、これ以上のさらなる著作物の不正使用を防止することが可能な著作権保護システムの実現が要望されている。

10

【0010】

また、放送番組の画像や音声など、放送により提供される著作物の著作権保護に関しては、その記録再生に対して対策がなされておらず、記録再生に係る著作権保護を実施可能な著作権保護システムの実現が要望されている。

【0011】

本発明は、このような事情を考慮してなされたもので、その目的は、自システム内の暗号に係る鍵を無効化することが可能な著作権保護システム及びその方法を提供することにある。また、その著作権保護システムをコンピュータを利用して実現するための著作権保護プログラムを提供することも目的とする。

20

【0012】

また、本発明は、複数の著作権保護システムにおいてそれらの暗号に係る鍵またはプログラムを簡易に変更することが可能な著作権保護システム及びその方法を提供することも目的とする。また、その著作権保護システムをコンピュータを利用して実現するための著作権保護プログラムを提供することも目的とする。

【0013】

また、本発明は、記録再生に係る著作権保護を実施可能な著作権保護システム及びその方法を提供することも目的とする。また、その著作権保護システムをコンピュータを利用して実現するための著作権保護プログラムを提供することも目的とする。

【0014】

【課題を解決するための手段】

30

上記の課題を解決するために、請求項1に記載の発明は、著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムであって、第1の暗号鍵を使用して前記入力データを暗号化し出力する第1の暗号化手段と、前記第1の暗号鍵を生成して前記第1の暗号化手段に提供し、認証鍵に基づいた相互認証の完了を条件として前記認証鍵を使用して前記第1の暗号鍵を暗号化し出力し、暗号に係る鍵の無効情報を有し、前記第1の暗号化手段と第1の暗号解除手段の間で前記第1の暗号鍵を共有する際の前記認証に使用する認証鍵の情報が前記無効情報の中に含まれる場合に、前記認証を不可とする認証手段と、前記入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する無効情報更新手段と、前記入力データに付随して提供される更新用認証鍵を受け取ると、前記認証鍵を更新する認証鍵更新手段とを具備することを特徴とする。

40

【0016】

請求項2に記載の発明は、前記暗号化の解除に係る機能を実現するための処理プログラムを実行する処理装置を備え、前記処理装置は、前記入力データに付随して提供される更新用プログラムを受け取ると、前記処理プログラムを更新することを特徴とする。

【0017】

請求項3に記載の発明は、第2の暗号鍵を使用して前記入力データを暗号化し、該第2の暗号データを記録媒体に記録する第2の暗号化手段を備えることを特徴とする。

【0018】

請求項4に記載の発明は、前記第2の暗号データの暗号を前記第2の暗号鍵により解除

50

する第2の暗号解除手段を備え、前記第2の暗号鍵を自システム内に保持することを特徴とする。

【0019】

請求項5に記載の発明は、著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムにおける著作権保護方法であって、第1の暗号鍵を生成する過程と、前記第1の暗号鍵を使用して前記入力データを暗号化し出力する第1の暗号化過程と、前記第1の暗号化を行う手段と第1の暗号解除手段の間で前記第1の暗号鍵を共有する際に、認証鍵に基づいた相互認証を行う過程と、この認証に使用する認証鍵の情報が暗号に係る鍵の無効情報の中に含まれる場合に、前記認証を不可とする過程と、前記認証の完了を条件として、前記認証鍵を使用して前記第1の暗号鍵を暗号化し出力する過程と、前記入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する過程と、前記入力データに付随して提供される更新用認証鍵を受け取ると、前記認証鍵を更新する過程とを含むことを特徴とする。

10

【0021】

請求項6に記載の発明は、前記入力データに付随して提供される更新用プログラムを受け取る過程と、この更新用プログラムにより、前記暗号化の解除に係る機能を実現するための処理プログラムを更新する過程とをさらに含むことを特徴とする。

【0022】

請求項7に記載の発明は、第2の暗号鍵を使用して前記入力データを暗号化する過程と、該第2の暗号データを記録媒体に記録する過程とをさらに含むことを特徴とする。

20

【0023】

請求項8に記載の発明は、前記第2の暗号鍵を自システム内に保持する過程と、前記第2の暗号データの暗号を自システム内に保持された第2の暗号鍵により解除する過程とをさらに含むことを特徴とする。

【0024】

請求項9に記載の発明は、著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムにおける著作権保護処理を行うための著作権保護プログラムであって、第1の暗号鍵を生成する処理と、前記第1の暗号鍵を使用して前記入力データを暗号化し出力する第1の暗号化処理と、前記第1の暗号化処理を行う手段と第1の暗号解除手段の間で前記第1の暗号鍵を共有する際に、認証鍵に基づいた相互認証を行う処理と、この認証に使用する認証鍵の情報が暗号に係る鍵の無効情報の中に含まれる場合に、前記認証を不可とする処理と、前記認証の完了を条件として、前記認証鍵を使用して前記第1の暗号鍵を暗号化し出力する処理と、前記入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する処理とをコンピュータに実行させることを特徴とする。

30

【0025】

請求項10に記載の発明は、第2の暗号鍵を使用して前記入力データを暗号化する処理と、該第2の暗号データを記録媒体に記録する処理と、をさらにコンピュータに実行させることを特徴とする。

【0026】

請求項11に記載の発明は、前記第2の暗号鍵を自システム内に保持する処理と、前記第2の暗号データの暗号を自システム内に保持された第2の暗号鍵により解除する処理と、をさらにコンピュータに実行させることを特徴とする。

40

【0027】

請求項12に記載の発明は、著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムにおける著作権保護処理を行うための著作権保護プログラムであって、前記入力データに付随して提供される更新用認証鍵を受け取り、認証鍵を更新する処理をコンピュータに実行させることを特徴とする。

【0028】

請求項13に記載の発明は、前記入力データに付随して提供される更新用プログラムを

50

受け取る処理と、この更新用プログラムにより、前記暗号化の解除に係る機能を実現するための処理プログラムを更新する処理とをさらにコンピュータに実行させることを特徴とする。

これらの著作権保護プログラムにより、前述の著作権保護システムがコンピュータを利用して実現できるようになる。

【0029】

【発明の実施の形態】

以下、図面を参照し、本発明の一実施形態について説明する。

図1は、本発明の一実施形態による著作権保護システムの構成を示すブロック図である。この図において、符号1は、放送信号を受信する放送受信装置である。この放送信号は、圧縮符号化され、さらに暗号化された画像データまたは音声データ（以下、圧縮暗号化データと称する）を含む。この暗号化は、視聴権利を有する者に対してのみ視聴可能とするためになされている。なお、上記放送信号は、テレビやラジオ等の無線放送やケーブルテレビ等の有線放送により伝送されるものであってもよく、あるいは、有線電話網や無線電話網、インターネット等の通信ネットワークを介して伝送されるものであってもよい。符号2は、放送受信装置1により受信された圧縮暗号化データの暗号を解除し、圧縮符号化された画像データまたは音声データ（以下、圧縮データと称する）を出力する放送暗号解除装置である。

【0030】

符号3は、放送暗号解除装置2から出力された圧縮データに対して第1の暗号鍵を使用して暗号化を行い、第1暗号データA1を出力する第1暗号化装置である。符号4は、第1の暗号鍵を生成して第1の暗号化装置3に提供し、また、認証鍵を使用して第1の暗号鍵を暗号化し、その認証鍵に基づいた相互認証の完了を条件として該暗号化された第1の暗号鍵を出力する認証装置である。この認証装置4は、無効な認証鍵の情報が記載された無効化鍵リストD1を有し、この無効化鍵リストD1の中に相互認証に使用する認証鍵の情報が含まれる場合には当該認証を不可とする。符号5は、放送信号に含まれる無効化対象の認証鍵の情報を放送受信装置1から受け取ると、その情報に基づいて認証装置4の無効化鍵リストD1を更新する無効鍵更新装置である。

【0031】

符号6は、メモリおよびCPU（中央処理装置）等により構成され、プログラムをメモリにロードして実行することによりその機能を実現する処理装置である。この処理装置6は、第1暗号解除部11と画像音声伸張部12と認証部13と認証鍵更新部14のそれぞれの機能を実現するためのプログラムを実行する。

【0032】

第1暗号解除部11は、第1暗号データA1を受け取り、当該暗号化に使用された第1の暗号鍵を使用してその暗号を解除する。画像音声伸張部12は、第1暗号解除部11によって暗号が解除された圧縮データを受け取り、このデータに対して伸張処理を行う。この伸張処理によって圧縮データは再生可能な画像データ及び音声データとなる。画像音声伸張部12は、伸張された画像データ及び音声データの再生処理も行うことが可能である。

【0033】

認証部13は、認証装置4との間でデータA2を送受して相互認証を行い、この認証完了により認証装置4から第1暗号解除部11で使用する第1の暗号鍵を取得する。この認証部13は、認証装置4との間の相互認証に使用する認証鍵を有している。認証鍵更新部14は、放送信号に含まれる更新用認証鍵を放送受信装置1から受け取ると、認証部13の認証鍵を更新する。また、認証鍵更新部14は、放送信号に含まれる更新用プログラムを放送受信装置1から受け取ると、第1暗号解除部11と画像音声伸張部12と認証部13と自部14のそれぞれの処理プログラム（第1の暗号解除処理プログラム、画像音声伸張処理プログラム、認証処理プログラム、認証鍵更新処理プログラム）を更新する。

【0034】

符号7は、放送暗号解除装置2から出力された圧縮データに対して第2の暗号鍵を使用し

て暗号化を行い、第2暗号データB1を出力する第2暗号化装置である。この第2暗号化装置7は、暗号化に使用した第2の暗号鍵を自装置内に保持する。符号8は、第2暗号化装置7から暗号化に使用された第2の暗号鍵を受け取り、その暗号を解除する第2暗号解除装置である。

【0035】

符号9は、第2暗号化装置7から第2暗号データB1を受け取ると、記録媒体に記録する記録装置である。この記録装置9としては、ハードディスク装置や光磁気ディスク装置、あるいはDVD (Digital Versatile Disc) 等の記録媒体の読み書き装置などが利用可能である。

【0036】

なお、上記処理装置6には、周辺機器として入力装置、表示装置、スピーカ等（いずれも図示せず）が接続されるものとする。ここで、入力装置とはキーボード、マウス等の入力デバイスのことをいう。表示装置とはCRT (Cathode Ray Tube) や液晶表示装置等のことをいう。このような処理装置6としては、パーソナルコンピュータや携帯情報端末などの情報処理装置が利用可能である。

【0037】

また、上記図1に示す装置の内、装置1～5、7及び8を一つの装置として構成するようにしてもよい。例えば、装置1～5、7及び8のそれぞれの機能を実現する電子回路を一つの基板上に実装し、これを処理装置6及び記録装置9と接続するようにする。このようにすれば、その基板をパーソナルコンピュータ等の情報処理装置に実装して図1の著作権保護システムを実現することが可能となる。

【0038】

なお、上記図1に示す装置3～5、7及び8は専用のハードウェアにより実現されるものであってもよい。また、それら装置3～5、7及び8はメモリおよびCPU (中央処理装置) により構成され、装置3～5、7及び8の各々の機能を実現するためのプログラムをメモリにロードして実行することによりその機能を実現させるものであってもよい。このようにCPU等からなるコンピュータを利用して実現する場合には、読出し専用のメモリ (ROM) にプログラムを格納するようにすれば、プログラムの改竄を防止することが可能である。あるいは、CPUやメモリ等を内蔵したLSI (システムLSI) により、それら装置3～5、7及び8を実現するようにしてもよい。

【0039】

次に、図1に示す著作権保護システムの動作を説明する。初めに、放送信号を受信してその放送内容を再生する動作について説明する。先ず、放送受信装置1は放送信号を受信すると、圧縮暗号化データを出力し、放送暗号解除装置2がその暗号を解除して圧縮データを出力する。

【0040】

次いで、第1暗号化装置3は、放送暗号解除装置2から圧縮データを受け取ると、認証装置4から提供された第1の暗号鍵を使用して暗号化を行い、第1暗号データA1を出力する。ここで使用される第1の暗号鍵は、処理装置6との間で共有される鍵である。なお、この第1の暗号鍵を共有する動作については後述する。

【0041】

次いで、処理装置6の第1暗号解除部11は、第1暗号化装置3から第1暗号データA1を受け取ると、第1暗号化装置3との間で共有された第1の暗号鍵を使用してその暗号を解除する。画像音声伸張部12は、第1暗号解除部11により暗号が解除された圧縮データを受け取ると、伸張処理を行い、画像または音声を再生する。

【0042】

上述したように本実施形態においては、第1暗号化装置3から処理装置6へ出力されるデータ (第1暗号データA1) は暗号化されたものなので、第1暗号化装置3と処理装置6の間を接続する伝送媒体 (データ伝送可能なバス等) からデータを取得しても、そのデータから再生可能な著作物のデータを取得することは困難である。

【0043】

次に、図2を参照して、上記第1の暗号鍵を共有する動作について説明する。この第1の暗号鍵の共有処理は認証装置4と認証部13の間で行われるが、その際、認証装置4と認証部13は認証鍵に基づいた相互認証を行う。図2は、第1の暗号鍵の共有処理の流れを示すフローチャートであって、公開鍵暗号方式による相互認証により第1の暗号鍵の共有する場合の例を示す。図2に示すように、認証装置4は、公開鍵p1、公開鍵証明書c1、秘密鍵s1、無効化鍵リストD1、及び公開鍵pcを有している。また、認証部13は、公開鍵p2、公開鍵証明書c2、秘密鍵s2、及び公開鍵pcを有している。

【0044】

上記公開鍵証明書c1は、第三者機関（認証局）により、この第三者機関（認証局）が有する秘密鍵scで予め公開鍵p1に署名が付加され発行されたものであり、この署名を公開鍵pcで検証する。同様に第三者機関により、公開鍵証明書c2は、秘密鍵scで予め公開鍵p2に署名が付加され発行されたものであり、この署名を公開鍵pcで検証する。これら署名により、公開鍵証明書c1、c2の偽造が防止される。

【0045】

公開鍵p1と秘密鍵s1は対を成す認証鍵である。同様に、公開鍵p2と秘密鍵s2も対を成す認証鍵となっている。なお、上記公開鍵p2と秘密鍵s2は、認証装置4と認証部13の間の相互認証に用いられる認証鍵の一つであり、認証装置4が行う第1の暗号鍵の暗号化に係る鍵となるものである。

また、無効化鍵リストD1には、無効な公開鍵証明書c2を示す情報が記載されている。この無効化鍵リストD1についても、偽造を防ぐために、第三者機関が有する秘密鍵scで署名が付加され発行される。

【0046】

まず、認証装置4は乱数R1を生成して認証部13へ送信する（図2のステップSP1、SP2）。次いで、認証部13は、受け取った乱数R1に対して秘密鍵s2で署名Sig(s2, R1 || ID2)を作成する。この署名Sig(s2, R1 || ID2)を作成する際には、番号ID2として公開鍵証明書c2のシリアル番号を用いるようにしてもよい。また、認証部13は乱数R2を生成する。次いで、認証部13は、作成した署名Sig(s2, R1 || ID2)と公開鍵証明書c2と乱数R2を認証装置4へ送信する（図2のステップSP3～SP5）。

【0047】

なお、上記記号「||」はビットの連結を示す。例えば、「R1 || ID2」は乱数R1と番号ID2がビット連結されたビット列を示し、署名Sig(s2, R1 || ID2)はそのビット列「R1 || ID2」に対して秘密鍵s2で署名が付加されたものである。

また、上記乱数R1、R2としては、熱雑音を使用してもよく、あるいは擬似乱数を使用してもよい。ただし、擬似乱数を使用する場合には、認証装置4と認証部13にそれぞれ擬似乱数生成器を備えるようにするが、それら擬似乱数生成器が不一致のものとなるようにする。

【0048】

次いで、認証装置4は、受け取った公開鍵証明書c2が無効化鍵リストD1に未記載であることを確認する。ここで、受け取った公開鍵証明書c2が無効化鍵リストD1に記載されていた場合には、認証装置4は、当該公開鍵p2が無効なものであると判断し、認証部13との認証を不可とし、認証未完了のままその処理を終了する。一方、受け取った公開鍵証明書c2が無効化鍵リストD1に未記載であった場合には、認証装置4は相互認証を継続し、以下の処理を行う（図2のステップSP6）。

【0049】

次いで、認証装置4は、公開鍵証明書c2を公開鍵pcで検証する。また、公開鍵p2と乱数R1により署名Sig(s2, R1 || ID2)を検証する。ここで認証装置4は、これら検証の結果がいずれか一つでも異常であった場合には、認証部13との認証を不可とし、認証未完了のままその処理を終了する（図2のステップSP7、SP8）。

【0050】

一方、認証装置4は、それら検証の結果が全て正常であった場合には、乱数R2に対して秘密鍵s1で署名Sig(s1, R2 || ID1)を作成する。この署名Sig(s1, R2 || ID1)を作成する際には、番号ID1として公開鍵証明書c1のシリアル番号を用いるようにしてもよい(図2のステップSP9)。

【0051】

次いで、認証装置4は、第1の暗号鍵K1を生成し、この第1の暗号鍵K1を公開鍵p2で暗号化して暗号Enc(p2, K1)を生成する。また、認証装置4は、その生成した第1の暗号鍵K1を第1暗号化装置3へ提供する。次いで、認証装置4は、署名Sig(s1, R2 || ID1)と公開鍵証明書c1と暗号Enc(p2, K1)を認証部13へ送信する(図2のステップSP10~SP12)。

10

【0052】

次いで、認証部13は、受け取った公開鍵証明書c1を公開鍵pcで検証する。また、公開鍵p1と乱数R2により署名Sig(s1, R2 || ID1)を検証する。ここで認証部13は、これら検証の結果がいずれか一つでも異常であった場合には、認証装置4との認証を不可とし、認証未完了のままその処理を終了する(図2のステップSP13、SP14)。

【0053】

一方、認証部13は、それら検証の結果が全て正常であった場合には、暗号Enc(p2, K1)を秘密鍵s2で復号して第1の暗号鍵K1を取得し、この第1の暗号鍵K1を第1暗号解除部11へ提供する(図2のステップSP15)。これにより、認証装置4によって生成された第1の暗号鍵K1が、第1暗号化装置3と第1暗号解除部11の間で共有されたことになる。

20

【0054】

なお、上述した実施形態においては、第1の暗号鍵の共有処理における認証を公開鍵暗号方式による相互認証により行うようにしたが、その認証方法は公開鍵暗号方式に限定されるものではない。

【0055】

次に、認証部13が有している認証鍵を無効化する動作を説明する。この無効化対象の認証鍵とは、認証装置4と認証部13の間の相互認証に用いられる認証鍵の一つであって、認証装置4が行う第1の暗号鍵の暗号化に係る鍵となるものである。上記図2に示す公開鍵暗号方式による相互認証の例においては、公開鍵p2と秘密鍵s2のことを指す。

30

【0056】

悪意を持った第三者が、図1の著作権保護システムの認証部13の認証鍵を不正に取得し、この認証鍵を用いて認証装置4と第1の暗号鍵を共有して第1暗号データA1の暗号を解除し、放送番組の画像や音声などの著作物を不正に使用する場合がある。このような場合には、放送事業者は、これ以上の著作物不正使用を防止するために無効化対象の認証鍵の情報と更新用認証鍵を放送信号に含めて放送する。以下、図1の著作権保護システムの動作を説明する。

【0057】

放送受信装置1は、受信した放送信号に無効化対象の認証鍵の情報が含まれている場合には、その情報を無効鍵更新装置5へ出力する。無効鍵更新装置5は、放送受信装置1から無効化対象の認証鍵の情報を受け取ると、この情報に基づいて認証装置4の無効化鍵リストD1を更新する。これにより、認証部13が有する認証鍵は無効化されたことになる。

40

【0058】

また、放送受信装置1は、受信した放送信号に更新用認証鍵が含まれている場合には、その更新用認証鍵を処理装置6の認証鍵更新部14へ出力する。認証鍵更新部14は、放送受信装置1から更新用認証鍵を受け取ると、認証部13の認証鍵を更新する。これにより、認証部13が有する認証鍵は有効な認証鍵となる。

【0059】

50

したがって、悪意を持った第三者が不正に取得した認証鍵により著作物を使用する場合には、認証装置４と認証部１３の間で第１の暗号鍵を共有する際に無効化された認証鍵が使用されることになるので、認証装置４は、上記図２のステップＳＰ６において認証部１３との間の相互認証を不可とし、第１の暗号鍵を認証部１３へ提供しない。この結果、第１暗号解除部１１は、第１暗号化装置３により暗号化に使用された第１の暗号鍵を取得することができず、第１暗号データＡ１の暗号を解除することができなくなる。これにより、たとえ悪意を持った第三者により、認証方式や暗号化方式が解読されて著作物が不正に使用されたとしても、認証鍵（暗号に係る鍵）を無効化して、これ以上のさらなる著作物の不正使用を防止することができるという効果が得られる。

【００６０】

また、上述したように本実施形態による著作権保護システムによれば、放送信号に含めて提供される無効化対象の認証鍵の情報と更新用認証鍵により、認証鍵の無効化とその変更を行う。したがって、放送事業者は、著作物の不正使用を防止するために無効化対象の認証鍵の情報と更新用認証鍵を放送信号に含めて放送するだけで、認証鍵の無効化とその変更を簡易に実施することができる。

【００６１】

このように、放送される画像データや音声データなどの著作物に係る入力データに付随して提供される無効化対象の認証鍵の情報や更新用認証鍵により、暗号に係る鍵（認証鍵）の無効化とその変更を行うようにすれば、当該著作物に係る入力データを使用する複数の著作権保護システムに対して、暗号に係る鍵の無効化とその変更を一斉に行うことが可能となる。この結果、当該著作物の不正使用に対する対処を能率よく実施することができるという効果が得られる。

【００６２】

また、放送事業者は、処理装置６の第１暗号解除部１１と画像音声伸張部１２と認証部１３と認証鍵更新部１４のそれぞれの処理プログラム（第１の暗号解除処理プログラム、画像音声伸張処理プログラム、認証処理プログラム、認証鍵更新処理プログラム）を更新可能な更新用プログラムを放送信号に含めて放送するようにしてもよい。この場合には、放送受信装置１は受信した更新用プログラムを認証鍵更新部１４へ出力し、認証鍵更新部１４がその更新用プログラムによりそれぞれの処理プログラムを更新する。このように処理装置６の処理プログラムを更新するようにすれば、当該処理プログラムが不正に改竄されて使用された場合においても、改竄された処理プログラムのさらなる不正使用を防止することが可能となる。

【００６３】

次に、図１に示す著作権保護システムが放送信号を受信してその放送内容を記録し、また記録された放送内容を再生する動作について説明する。まず、放送受信装置１は放送信号を受信すると、圧縮暗号化データを出力し、放送暗号解除装置２がその暗号を解除して圧縮データを出力する。

【００６４】

次いで、第２暗号化装置７は、放送暗号解除装置２から圧縮データを受け取ると、第２の暗号鍵を使用して暗号化を行い、第２暗号データＢ１を出力する。第２暗号化装置７は、暗号化の契機がある度に乱数等を利用して第２の暗号鍵を生成し、自装置７内に保持する。記録装置９は、第２暗号化装置７から第２暗号データＢ１を受け取ると、記録媒体へ記録する。

【００６５】

この記録されたデータを再生する場合には、まず、記録装置９が記録媒体から第２暗号データＢ２を読み出して出力する。第２暗号解除装置８は、この第２暗号データＢ２を受け取ると、その暗号化に使用された第２の暗号鍵を第２暗号化装置７から取得し、第２暗号データＢ２の暗号を解除して第１暗号化装置３へ出力する。次いで、上述した第１の暗号鍵による暗号化に係る過程を経た後、画像音声伸張部１２によって、記録装置９により記録された放送内容が再生されることになる。

10

20

30

40

50

【0066】

なお、上述した実施形態においては、第2暗号解除装置8への第2の暗号鍵の提供方法として、第2暗号化装置7が暗号化の契機がある度に乱数等を利用して第2の暗号鍵を生成し、この第2の暗号鍵を自装置7内に保持するようにしたが、第2の暗号鍵を記録装置9により記録するようにしてもよい。ただし、この場合には、自システムにおいてのみその記録した第2の暗号鍵を使用可能となるようにする。例えば、第2暗号化装置7毎に異なる固有のID（識別番号）と、第2の暗号鍵との所定演算の結果を第2暗号データB1に付加して記録する。この場合には、第2暗号解除装置8は、第2暗号化装置7からそのIDを取得し、第2暗号データB1に付加された演算結果と取得したIDにより、第2の暗号鍵を復元して取得する。

10

【0067】

上記いずれかの第2の暗号鍵の提供方法により第2の暗号鍵を第2暗号解除装置8に提供するようにしておけば、たとえ図1に示す著作権保護システムから記録装置9を取り外して同様の構成を備えた他の著作権保護システムに取り付けたとしても、正しい第2の暗号鍵を得ることは困難であり、記録した著作権保護システム以外のシステムでは再生不可とすることができるようになる。この結果、著作物そのものが不正に複製されることを抑止するという効果が得られる。

【0068】

なお、上記いずれかの第2の暗号鍵の提供方法により、記録した著作権保護システム以外のシステムでは再生不可とするようにしておいてもよいし、あるいは他の方法を用いてもよい。例えば、記録媒体からの読出し自体にシステム固有の認証を必要とするようにしてもよい。

20

【0069】

また、上述した実施形態によれば、記録に係る装置7～9と再生に係る装置3～6とを独立に備えるようにしたので、記録処理と再生処理を同時におこなうタイムシフトと呼ばれる処理も行うことができる。

【0070】

上述したように本実施形態によれば、記録時の暗号化方式（第2の暗号鍵による方式）と再生時の暗号化方式（第1の暗号鍵による方式）にそれぞれ異なる方式を用いるようにしたので、たとえ再生時の第1の暗号が解読され、著作物の記録または再生が不正に行われたとしても、記録時の第2の暗号が直接解読されることを防止することは可能である。したがって、再生時の第1の暗号に係る鍵（認証鍵）を変更することによって、これ以上は不正に著作物が記録または再生されることを防止することができる。また、第2の暗号で記録されたデータについては、以前と同様に再生が可能である。

30

この結果、利用者の利便性を損なうことなく、記録再生に係る著作権保護を実施することができるという効果が得られる。

【0071】

なお、上述した実施形態においては、著作権保護対象の著作物を画像または音声とし、暗号化対象の著作物に係る入力データとして画像データまたは音声データを例にして説明したが、他の著作物に対しても同様に適用可能である。例えば、小説等の文章を著作権保護対象の著作物とする場合には、著作物に係る入力データをテキストデータとして適用すればよい。

40

【0072】

また、上述した実施形態においては、著作物に係る入力データを放送信号に含めて配信する場合について説明したが、著作物に係る入力データの取得方法は、放送形式で配信される場合に限定されるものではない。例えば、著作権保護システムの利用者がインターネット等の通信ネットワークを介して著作物に係る入力データを自ら取得するようにしてもよい。この場合には、図1の装置1、2の代わりに、通信ネットワーク接続装置（モデムやダイヤルアップルータ等）とその通信データに係る暗号解除装置を備えるようにする。

【0073】

50

あるいは、著作物に係る入力データを記録媒体を介して取得するようにしてもよい。例えば、DVDに記録された著作物のデータを著作物に係る入力データとしてもよい。この場合には、図1の装置1、2の代わりに、DVDの読出し装置とその読出しデータに係る暗号解除装置を備えるようにする。

【0074】

なお、上述した実施形態においては、図1の第1暗号化装置3が第1の暗号化手段に対応し、第1暗号解除部11が第1の暗号解除手段に対応する。また、認証装置4が認証手段に対応し、認証装置4の無効化鍵リストD1の記載内容が暗号に係る鍵の無効情報に対応する。また、無効鍵更新装置5が無効情報更新手段に対応する。

【0075】

また、処理装置6の認証鍵更新部14が認証鍵更新手段に対応する。また、処理装置6が暗号化の解除に係る機能を実現するための処理プログラムを実行する処理装置に対応する。また、第1暗号解除部11と画像音声伸張部12と認証部13と認証鍵更新部14のそれぞれの処理プログラム（第1の暗号解除処理プログラム、画像音声伸張処理プログラム、認証処理プログラム、認証鍵更新処理プログラム）が暗号化の解除に係る機能を実現するための処理プログラムに対応する。

【0076】

また、第2暗号化装置7が第2の暗号化手段に対応し、第2暗号解除装置8が第2の暗号解除手段に対応する。

【0077】

また、図1に示す装置3～8が行う各処理を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより著作権保護処理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、OSや周辺機器等のハードウェアを含むものであってもよい。

また、「コンピュータシステム」は、WWWシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。

また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ROM、CD-ROM、メモリカード等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

【0078】

さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（RAM）のように、一定時間プログラムを保持しているものも含むものとする。

また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【0079】

以上、本発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等も含まれる。

【0080】

【発明の効果】

以上説明したように、本発明によれば、第1の暗号鍵を生成し、該第1の暗号鍵を使用して著作物に係る入力データを暗号化し出力し、認証鍵に基づいた相互認証の完了を条件

10

20

30

40

50

として前記認証鍵を使用して前記第1の暗号鍵を暗号化し出力し、暗号に係る鍵の無効情報を有し、第1の暗号化手段と第1の暗号解除手段の間で第1の暗号鍵を共有する際の認証に使用する認証鍵の情報が無効情報の中に含まれる場合に、当該認証を不可とする。また、著作物に係る入力データに付随して提供される無効化対象の鍵の情報を受け取ると、無効情報の内容を更新する。これにより、自システム内の暗号に係る鍵を無効化することが可能となる。さらに、著作物に係る入力データを使用する複数の著作権保護システムに対して、暗号に係る鍵の無効化を一斉に行うことが可能となる。この結果、著作物の不正使用に対する対処を能率よく実施することができるという効果も得られる。さらに、著作物に係る入力データに付随して提供される更新用認証鍵により、認証鍵を更新するので、複数の著作権保護システムにおいてそれらの暗号に係る鍵（認証鍵）を簡易に変更することができる。

10

【0082】

また、著作物に係る入力データに付随して提供される更新用プログラムを受け取り、この更新用プログラムにより、暗号化の解除に係る機能を実現するための処理プログラムを更新するようにすれば、複数の著作権保護システムにおいてそれらの暗号に係るプログラムを簡易に変更することができる。

【0083】

また、第2の暗号鍵を使用して著作物に係る入力データを暗号化し、該第2の暗号データを記録媒体に記録するようにすれば、記録時の暗号化方式（第2の暗号鍵による方式）と再生時の暗号化方式（第1の暗号鍵による方式）にそれぞれ異なる方式を用いることが可能となり、たとえ再生時の第1の暗号が解読され、著作物の記録または再生が不正に行われたとしても、記録時の第2の暗号が直接解読されることを防止することは可能である。したがって、再生時の第1の暗号に係る鍵（認証鍵）を変更することによって、これ以上は不正に著作物が記録または再生されることを防止することができる。また、第2の暗号で記録されたデータについては、以前と同様に再生が可能である。この結果、利用者の利便性を損なうことなく、記録再生に係る著作権保護を実施することができるという効果が得られる。

20

【0084】

さらに、第2の暗号鍵を自システム内に保持し、第2の暗号データの暗号を自システム内に保持された第2の暗号鍵により解除するようにすれば、著作物を記録した著作権保護システム以外のシステムではその記録データを再生不可とすることができるようになる。この結果、著作物そのものが不正に複製されることを抑止するという効果が得られる。

30

【図面の簡単な説明】

【図1】 本発明の一実施形態による著作権保護システムの構成を示すブロック図である。

【図2】 図1に示す著作権保護システムが行う第1の暗号鍵の共有処理の流れを示すフローチャートである。

【図3】 従来の著作権保護システムの構成例を示すブロック図である。

【符号の説明】

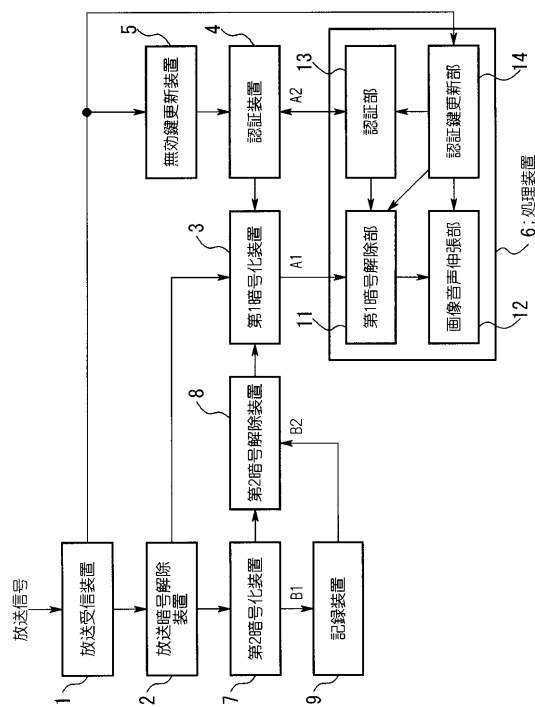
- 1 放送受信装置
- 2 放送暗号解除装置
- 3 第1暗号化装置
- 4 認証装置
- 5 無効鍵更新装置
- 6 処理装置
- 7 第2暗号化装置
- 8 第2暗号解除装置
- 9 記録装置
- 11 第1暗号解除部
- 12 画像音声伸張部

40

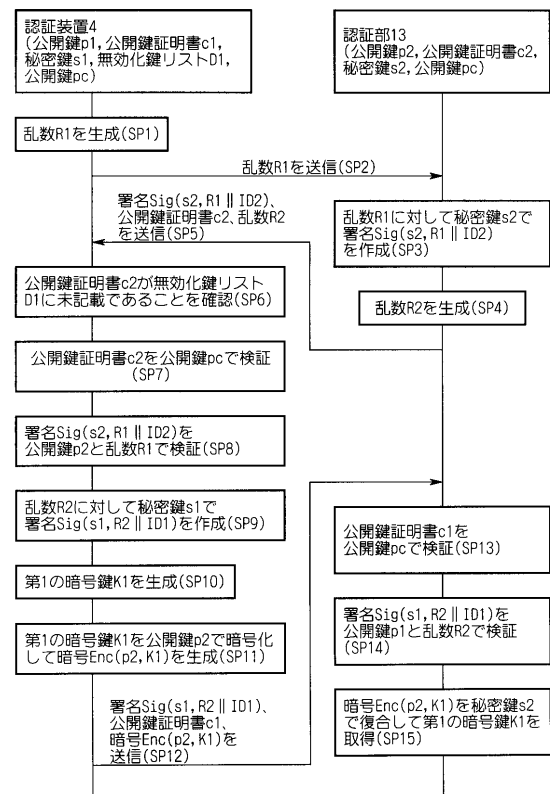
50

- 1 3 認証部
 1 4 認証鍵更新部
 D 1 無効化鍵リスト

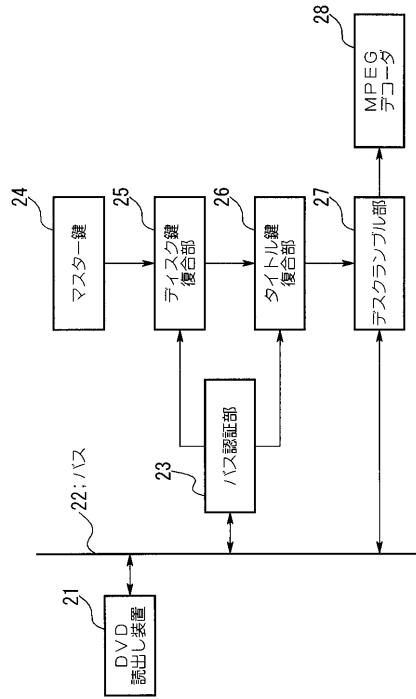
【図 1】



【図 2】



【図 3】



フロントページの続き

- (72)発明者 峯松 一彦
東京都港区芝五丁目7番1号 日本電気株式会社内
- (72)発明者 尾花 賢
東京都港区芝五丁目7番1号 日本電気株式会社内

合議体
審判長 吉岡 浩
審判官 野仲 松男
審判官 富吉 伸弥

- (56)参考文献 米国特許第5949877 (US, A)
特開平11-161165 (JP, A)
特開平8-23313 (JP, A)
特開2000-31922 (JP, A)
5C Digital Transmission Content Protection
White Paper, Revision 1.0, 1998年7月14日

- (58)調査した分野(Int.Cl., DB名)
H04L9/00