(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4921377号
(P4921377)

(45)発行日　平成24年4月25日(2012.4.25)　(24)登録日　平成24年2月10日(2012.2.10)

(51)Int.Cl.		F I		
G06F 21/22	(2006.01)	G06F	21/22	110L
G06F 21/24	(2006.01)	G06F	21/24	165F
H04L 9/32	(2006.01)	H04L	9/00	673D
H04N 1/387	(2006.01)	H04N	1/387	
G06T 1/00	(2006.01)	G06T	1/00	500B

請求項の数 10　(全 11 頁)　最終頁に続く

(21)出願番号　特願2007-542458 (P2007-542458)
(86)(22)出願日　平成17年11月21日 (2005.11.21)
(65)公表番号　特表2008-521121 (P2008-521121A)
(43)公表日　平成20年6月19日 (2008.6.19)
(86)国際出願番号　PCT/IB2005/053847
(87)国際公開番号　WO2006/056938
(87)国際公開日　平成18年6月1日 (2006.6.1)
審査請求日　平成20年11月19日 (2008.11.19)
(31)優先権主張番号　60/630,670
(32)優先日　平成16年11月24日 (2004.11.24)
(33)優先権主張国　米国 (US)

前置審査

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　ギュッタ，スリニヴァス　ヴェンカータラーマ
オランダ国，５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1

最終頁に続く

(54)【発明の名称】セキュリティスコアに基づく復号／暗号解読

(57)【特許請求の範囲】
【請求項１】
保護されたコンテンツ素材の再生を制御する方法であって：
前記保護されたコンテンツ素材の電子透かしとして埋め込まれたセキュリティ情報である許可ディスクのシリアル番号と、前記コンテンツ素材に関連付けられた認証情報である、前記コンテンツ素材が取得されたディスクのシリアル番号との一致ビット数に基づき、セキュリティスコアを決定する段階；
前記コンテンツ素材に関連付けられたメタデータに基づき、セキュリティ基準を決定する段階；及び
前記セキュリティスコアと前記セキュリティ基準との間の比較に基づき、前記コンテンツ素材の再生を制御する段階、
を有する方法。
【請求項２】
前記セキュリティ基準は：
前記コンテンツ素材の著作権の登録の日付、
前記コンテンツ素材のランキング、
前記コンテンツ素材に関連付けられた人物、
の少なくとも１つを有し、
前記コンテンツ素材に関連付けられたメタデータに基づく、
ことを特徴とする請求項１記載の方法。

【請求項３】
前記認証情報は前記コンテンツ素材を有する媒体と関連付けられた情報に対応する、
ことを特徴とする請求項１記載の方法。
【請求項４】
前記再生を制御する段階は、前記コンテンツ素材の再生の品質を制御する段階を有する、
ことを特徴とする請求項１記載の方法。
【請求項５】
前記セキュリティ基準は前記コンテンツ素材と共に提供される、
ことを特徴とする請求項１記載の方法。
【請求項６】
保護されたコンテンツ素材を受信するよう構成された受信機；
前記コンテンツ素材を復号し再生可能コンテンツ素材を提供するよう構成された復号器；
前記受信機と機能するよう結合され、前記保護されたコンテンツ素材の電子透かしとして埋め込まれたセキュリティ情報である許可ディスクのシリアル番号と、前記コンテンツ素材に関連付けられた認証情報である、前記コンテンツ素材が取得されたディスクのシリアル番号との一致ビット数に基づき、セキュリティスコアを決定するよう構成されたセキュリティ評価器；
前記セキュリティ評価器に機能するよう結合され、前記コンテンツ素材に関連付けられたメタデータに基づきセキュリティ基準を決定し、及び前記セキュリティスコア及び前記セキュリティ基準の比較に基づき前記復号器を制御するよう構成されたセキュリティ制御部、
を有するシステム。
【請求項７】
前記セキュリティ基準は：
前記コンテンツ素材の著作権の登録の日付、
前記コンテンツ素材のランキング、
前記コンテンツ素材に関連付けられた人物、
の少なくとも１つに基づく、
ことを特徴とする請求項６記載のシステム。
【請求項８】
前記復号器は、前記再生可能コンテンツ素材の品質を変化するよう制御可能であり、
前記セキュリティ制御部は、前記セキュリティスコアと前記セキュリティ基準との間の比較に基づき、前記評価器において前記品質を制御するよう構成される、
ことを特徴とする請求項６記載のシステム。
【請求項９】
前記セキュリティ基準は、調整可能なセキュリティレベルを有する、
ことを特徴とする請求項１記載の方法。
【請求項１０】
前記セキュリティ基準は、調整可能なセキュリティレベルを有する、
ことを特徴とする請求項６記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子セキュリティシステム、及び特に保護コンテンツ素材の受信機により決定されるセキュリティスコアに基づき復号又は暗号解読処理を制御するコピー／再生防止システムに関する。
【背景技術】
【０００２】

著作権素材を不正コピー及び分配から保護する防止システムの必要は、増大し続けている。同時に、このような防止システムの信頼性への不満は、これらシステムの実施を妨げている。

【０００３】

特に懸念されることは、防止システムがコンテンツ素材の許可されたコピーの再生を拒否するという「偽陰性」の問題である。消費者は、許可素材の再生を拒否する製品に対し非常に不満を抱く。また許可素材の再生を妨げるという評判を得た製品のベンダーは、将来の製品の売り上げを含むかなりの売り上げを失う可能性がある。同様に、許可素材を再生させるまで長時間を要するという評判を得た製品は、ベンダーの売り上げに影響を及ぼすだろう。

【０００４】

反対に、防止システムが無許可素材を再生させる「偽陽性」の問題は、許可コンテンツ素材の売り上げに影響を及ぼす。また偽陽性を高い率で示すシステムは、コンテンツプロバイダーの推薦を受けないだろう。

【０００５】

共通セキュリティ技術の例及びそれらの制限の例は次の通りである。

【０００６】

透かしは、コンテンツ素材を保護するために一般的に用いられる。透かしは、透かしの除去が保護素材の品質に不利に影響を及ぼさず、更に透かしの存在が素材の品質に不利に影響を及ぼさないよう、設計される。大部分の防止システムでは、透かしは、素材のその時のコピーが有効なコピーか否かを決定するために復号されなければならない情報を有する。透かしは実質的に「不可視」でなければならないので、透かし信号の大きさは、素材の大きさより実質的に小さくなければならない。また透かし内に含まれる情報の復号化は、特に素材の情報源と透かし検出器の間の素材の処理が透かし信号の大きさのレベルにおいて又はそのレベル近くの雑音を導入する場合、誤りの影響を受けやすい。

【０００７】

透かし信号の潜在的信号対雑音比を向上するため、いくつかの防止システムは実質的に透かし信号の帯域を削減している。しかしながら、このような削減は、透かしに含まれ得る情報量を制限し、及び／又は透かしを受信し素材が許可されているか否かを決定するために要する時間を増加する。代案として、複数の透かしが素材中に符号化されて良い。そして素材へのアクセスの許可は、認証に成功した透かしの比率に基づく。

【０００８】

バイオメトリック指標はまた、保護されたコンテンツ素材へのアクセスを制御するために提案されている。標準的に、バイオメトリック特徴は検知装置により検知され又はサンプルを採られる。そしてサンプルに関連付けられたパラメーターは、バイオメトリック特徴の他のサンプルと関連付けられたパラメーターと比較するために格納される。参照を簡単にするため、バイオメトリック又はバイオメトリック指標の語は、以後、検知された又はサンプルを採られたバイオメトリック特徴に関連付けられたパラメーターを参照するために用いられる。従って、例えば、「指紋」の語は、標準的に個人の指先の画像から引き出される如何なるパラメーターも含む。例であるバイオメトリックセキュリティシステムでは、購入者の指紋は、コンテンツ素材が購入された場合、コンテンツ素材を暗号化するための鍵を生成するために用いられる。このようなシステムでは、受信装置は、ユーザーの指紋に基づきコンテンツ素材を解読するための鍵を同様に生成するよう構成される。暗号鍵と復号鍵の生成に同一の指が用いられる場合、暗号化された素材は受信装置において正しく解読される。

【０００９】

別の例であるバイオメトリックセキュリティシステムでは、購入者の指紋（又は他のバイオメトリック特徴）は、コンテンツ素材の購入されたコピーに埋め込まれる透かしに符号化される。受信システムは透かしを復号し、購入者の指紋をユーザーの指紋と比較し、そしてその次に指紋が一致した場合のみ保護素材を再生する。

【００１０】
良く知られていることに、しかしながら、バイオメトリクスは時間に伴い変化し、各バイオメトリックの読み取りは、用いられる特定の装置、送信装置に関連するバイオメトリック特徴の方向、バイオメトリック特徴と送信装置との間のインターフェースのレベル、バイオメトリック特徴の明瞭さ、等に基づき異なり得る。犯罪法医学の分野で知られているように、例えば、個人の指紋の異なるインスタンスに存在する不一致は、一致を断言するために専門家の分析を必要とする。
【００１１】
他の技術はまた、保護素材へのアクセスを制御するために利用可能である。これら技術の何れも絶対信頼できると示されていない。それぞれの知られている技術は、ある誤りの可能性を示し、この誤りは２つの要素を有する。つまり、偽陽性（無許可素材を見せる）及び偽陰性（許可素材を見せることを妨げる）である。誤りの可能性は、試験と関連付けられた（例えば前述の、信号対雑音比を向上するための透かし帯域の削減）、しかし標準的に不利な副作用を伴う（例えば前述の、透かし処理時間が長い及び／又は透かし情報コンテンツが削減される）パラメーターを変更することにより制御され得る。更に、従来知られているように、１つの誤り成分（偽陽性又は偽陰性）の削減は、一般的に他の誤り成分の増加をもたらす。
【００１２】
全ての知られているセキュリティシステムが誤りの可能性を示すならば、このような誤りの影響を制御する必要が存在する。
【発明の開示】
【発明が解決しようとする課題】
【００１３】
本発明の目的は、偽陰性及び偽陽性の可能性を動的に制御することである。本発明の更なる目的は、素材が許可素材であるという信頼の指標に基づき、コンテンツ素材の再生を動的に制御することである。本発明の更なる目的は、再生されている素材に関連する因子に基づき、コンテンツ素材の再生を動的に制御することである。
【課題を解決するための手段】
【００１４】
これら及び他の目的は、受信コンテンツ素材が再生されることを許可される可能性に相当するセキュリティスコアを提供し、及びセキュリティスコアに基づき素材の再生を制御する方法及びシステムにより達成される。セキュリティスコアは、異なる素材が異なる制限を課すよう、再生されている素材と関連付けられたセキュリティ基準と比較され得る。セキュリティスコアはまた、素材の再生の品質／忠実度のレベルを制限し得る。従って例えば、素材の高い忠実度の（ハイファイ）コピーは、コピーの提供が許可される高度の信頼性が確立された場合のみ提供される。
【発明を実施するための最良の形態】
【００１５】
本発明の実施例は、例として以下の図を参照し詳細に説明される。
【００１６】
図中、同一の参照符号は同一の要素又は実質的に同一の機能を実行する要素を参照する。図は説明を目的とし、本発明を限定するものと見なされるべきではない。
【００１７】
図１は、本発明によるセキュリティシステムの例であるブロック図を図示す。セキュリティシステムは、保護コンテンツ１０１を受信する受信機１１０、保護コンテンツを再生可能形式に変換する復号器１４０、コンテンツ素材１０１と関連付けられたセキュリティ指標１２５を決定するセキュリティ評価器１２０、及び復号器１４０をセキュリティ指標１２５に基づき制御するセキュリティ制御部１５０を有する。
【００１８】
復号器１４０は、素材１０１の制御可能な再生を提供するために用いられる如何なる種

類の装置も有する。コンテンツ素材１０１の暗号化形式を用いる実施例では、例えば、復号器１４０は、制御部１５０により提供される情報に基づき素材を解読するよう構成された解読器を有する。別の又は補足の実施例では、復号器１４０は、制御部１５０により有効に又は無効にされるよう構成されて良く、又は以下に議論されるように制御部１５０からの制御信号に基づき出力の忠実度／品質の変化する程度を提供するよう構成されて良い。

【００１９】

図１の例では、セキュリティ評価器１２０は、セキュリティ情報１１５を受信するよう構成される。セキュリティ情報１１５は、例えば透かしに基づくセキュリティシステムで用いられ得るように、受信機１１０からのコンテンツ素材に含まれている。更に、セキュリティ評価器１２０は、認証情報１２１を受信する。認証情報１２１は、セキュリティ情報１１５に基づきコンテンツ素材１０１の認証を検証するために用いられる。例えば、許可ディスクのシリアル番号を有する透かしは、素材１０１に埋め込まれて良い。受信機１１０は、セキュリティ評価器１２０へこの透かしをセキュリティ情報１１５として提供するよう構成される。また、コンテンツ素材１０１を提供するディスクドライブ（図示されない）は、素材１０１が取得されたディスクのシリアル番号を認証情報１２１として提供する。

【００２０】

セキュリティ評価器１２０は、適切な試験を適用し、従来一般的な技術を用いコンテンツ素材１０１が許可されている／有効であるか否かを決定する。従来のセキュリティシステムと対照的に、しかしながら、本発明のセキュリティ評価器１２０は、従来の２値の合格／不合格の決定ではなく定量的スコア１２５を提供する。例えば、認証がシリアル番号の比較に基づく場合、スコア１２５は、透かしからのシリアル番号の復号化が誤りを発生し易いことを認識して、シリアル番号の一致ビット数に基づいて良い。同様の方法で、認証がバイオメトリクスの比較に基づく場合、スコア１２５は、バイオメトリクスの間の一致の程度、例えば指紋の対において一致する特徴点の数に基づいて良い。

【００２１】

前述の標準的に透かしに関連付けられた低信号対雑音比のため、及び／又は前述のバイオメトリクスの変動の高さのため、保護コンテンツ素材１０１は、しばしばセキュリティ情報１１５と共に重複して符号化される。また、多くのセキュリティシステムでは、複数のしかし必ずしも重複しないセキュリティ識別子が用いられ、素材１０１の有効性を継続的に検査する手段を提供する。定量的スコアを提供する別の例では、特定の試験が２値の結果のみを提供する場合でさえ、セキュリティ評価器１２０は、合格又は不合格である試験の比率に基づく、及び／又は多数の試験の平均スコアに基づくセキュリティスコア１２５を提供するよう構成され得る。保護素材に関連付けられたセキュリティ情報に基づくセキュリティスコアを提供するこれら及び他の技術は、この開示を閲覧する当業者には明らかである。

【００２２】

本発明の第１の態様によると、セキュリティ制御部１５０は、セキュリティ評価器１２０からのセキュリティスコア１２５、及びセキュリティ基準１５１を用い、復号器１４０を制御する。このセキュリティ基準１５１は、以下に詳細に説明されるように種々の形式を取り得る。しかし、基準１５１の主要目的は、コンテンツ素材１０１と関連付けられた情報に基づき、セキュリティ制御部１５０に復号器１４０を動的に制御させることである。本発明の目的のため、動的制御の語は、異なる時刻における異なる制御を提供することを有する。異なる制御は、同一のコンテンツ素材１０１が処理されている間に適用されて良く、又はコンテンツ素材１０１の異なるインスタンスに適用されて良い。

【００２３】

セキュリティ基準１５１の第１の例では、コンテンツ素材１０１のプロバイダーは、最低限必要なセキュリティレベルをコンテンツ素材１０１に関連付けて良い。ここでレベルが高いほど、素材１０１の再生にかかる制御は厳しい。セキュリティスコア１２５が最低

限必要なセキュリティレベルより上である場合、セキュリティ制御部１５０は、復号器１４０にコンテンツ素材１０１の再生を継続させる。その他の場合、再生は終了させられる。

【００２４】

セキュリティ評価器１２０が素材１０１に関連付けられた現行のスコアを、例えば繰り返し試験又は連続試験に基づき提供するよう構成される場合、セキュリティ制御部１５０は、セキュリティスコアが当該コンテンツ素材１０１と関連付けられた最低レベルより下に落ちた場合はいつでも再生を終了するよう構成されて良い。代案として、プロバイダーは、基準１５１のセット、例えば再生を開始するために必要な初期レベル及び特定点を超えて継続するために必要なより高いレベルをコンテンツ素材１０１に関連付けて良い。この方法では、素材の再生を開始する際の遅延時間は削減され得ると同時に、依然としてコンテンツ素材のかなりの部分を再生するために高レベルのセキュリティが保証される。

【００２５】

更に別の実施例では、正式な統計的試験は、セキュリティ制御部１５０により適用されて良い。またプロバイダーは、合格／不合格の基準、例えば再生を終了するために必要な信頼レベルを試験結果に関連付けて良い。セキュリティ評価器１２０による複数の連続評価の例では、逐次試験、例えば逐次確率比検定（ＳＰＲＴ）の使用は、再生を許可するか、試験を継続するか、又は再生を防止するかの決定に特に良く適する。

【００２６】

特に留意すべき点は、本発明によると、異なる基準１５１が異なるコンテンツ素材１０１に関連付けられ得ることである。この方法では、コンテンツ素材１０１のプロバイダーは、前述の偽陰性及び偽陽性の誤り率を効率的に制御し得る。プロバイダーが、厳格な制御で顧客を悩ませる可能性及び偽陰性の可能性のコストより不正コピーのコストが重要であると考える場合、プロバイダーはセキュリティ基準１５１を高く設定し得る。一方、プロバイダーが再生困難な素材１０１を販売するという評判を得ることを懸念する場合、プロバイダーは、無許可素材の再生を認める可能性は増大するが、より低い基準１５１を選択し偽陰性の可能性を低減して良い。

【００２７】

本発明の使用により、著作権の施行により最も影響を受ける団体は、この施行に付属する利点及び不利点とともにこの施行の制御を提供される。また、再生機器のベンダーは、偽陰性と偽陽性の誤りの間の適切な平衡を決定する負担から開放される。代案として、プロバイダーがこの負担の受け入れ及びセキュリティ基準の設定を嫌がる場合、機器のベンダーはこの機能を用い、実際の実地試験及びユーザーのフィードバックに基づき偽陰性の許容可能な程度を達成するためセキュリティレベルを調整し得る。同様に、コンテンツ素材１０１の異なるプロバイダーがセキュリティ情報１１５の信頼性の異なるレベル、例えば異なるレベルの信号対雑音比を示し得る場合、再生機器のベンダーは、素材１０１のプロバイダーに基づき異なるレベルのセキュリティを実行するよう選択し、ベンダーの再生機器に起因するセキュリティ情報１１５の欠陥を有することを回避し得る。

【００２８】

更に、本発明の使用により、コンテンツ情報１０１のプロバイダーは、無許可素材の再生の許可による期待損失が低減されるので、許可素材の再生を妨げる可能性を低減する機能を提供される。例えば、不正コピーが利用可能である場合、トップにランキングされた映画が分配のために最初に公開される時の映画の許可コピーの売り上げからの利益損失は、相当量であり得る。他方で、分配後１年又は２年の期待利益は実質的に少なく、及び従って不正コピーへの利益の期待損失はそれに応じて少ない。同様の方法で、下位にランキングされた映画の期待利益は、トップにランキングされた映画からの期待利益より実質的に少ない。及び従って下位にランキングされた映画の不正コピーへの利益の期待損失は、トップにランキングされた映画の不正コピーへの損失より実質的に少ないだろう。本発明の使用により、コンテンツ素材１０１のプロバイダーは、特定のコンテンツ素材１０１の利益の期待損失に基づき基準１５１を変更し得る。同様の方法で、素材１０１のプロバイ

ダーがセキュリティ基準１５１を提供しない場合、受信機器のベンダーは、素材１０１の時機、素材１０１のランキング、等に基づき異なる基準１５１を実施するよう選択し得る。

【００２９】

如何なる種々の方法も、セキュリティ基準１５１をセキュリティ制御部１５０へ通信するために用いられて良い。簡単な実施例では、セキュリティ基準１５１は、コンテンツ素材１０１と共に提供されるメタ情報内に含まれて良い。例えば、セキュリティ基準１５１は、標準的にＣＤ及びＤＶＤに設けられるコンテンツのテーブル、又は放送伝送で提供される概要に含まれて良い。代案の実施例では、セキュリティ基準１５１は、素材１０１のプロバイダー、受信機器のベンダー、又はベンダー又はオーディオ製作者の団体のような第三者と関連付けられたウェブサイトとのオンライン接続を介し得られて良い。

【００３０】

ベンダーの決定するセキュリティ基準１５１、又は製品の決定するセキュリティ基準１５１のシナリオの例では、セキュリティ基準１５１は現在の日付に基づいて良く、及びセキュリティ制御部１５０は現在の日付とコンテンツ素材１０１と関連付けられた日付、例えば素材１０１と関連付けられたメタデータ内で見付かった著作権登録日付との間の差に基づき、復号器１４０を制御するよう構成される。例えば素材１０１が１年未満の古さの場合、セキュリティ制御部１５０は、非常に高いセキュリティスコア１２５が達成されるまで素材１０１の再生を防止するよう構成されて良い。他方で、素材１０１が１０年の古さの場合、制御部１５０は、セキュリティスコア１２５が低い場合でさえ素材１０１の再生を許可して良い。同様に、セキュリティ制御部１５０は、現在の人気俳優及び女優、現在の人気プロデューサー及びディレクターの名前、等のような「人気」項目を有するメモリーを有して良い。このような実施例では、セキュリティ基準１５１は、素材１０１と関連付けられたメタデータであって良い。また制御部１５０がメタデータと「人気」項目との間の一致を検出する場合、より高レベルのセキュリティスコア１２５が、素材１０１の再生を認めるために要求される。

【００３１】

別の例である実施例では、セキュリティ基準１５１は、復号器１４０により提供される機能に依存して良い。つまり、例えば、素材１０１のコピーを生成するためのセキュリティ基準１５１は、素材１０１を単に再生するためのセキュリティ基準より実質的に高く設定されて良い。この方法では、復号器１４０を用い保護素材１０１を再生するユーザーは、復号器１４０を用い素材１０１のコピーを生成するユーザーより、偽陰性の決定による影響を受ける可能性が低い。

【００３２】

セキュリティスコア１２５に基づく再生制御の決定が基づくセキュリティ基準１５１を定義し及び決定するこれら及び他の方法は、本開示を閲覧する当業者に明らかである。

【００３３】

図２は、図１のセキュリティシステムで用いられて良い、本発明による保護コンテンツ素材の再生を動的に制御するセキュリティシステムの例であるフロー図を図示す。

【００３４】

２１０において、セキュリティ基準は、例えば上述の方法の１つを用い決定される。図示されないが、セキュリティ基準が無い場合、図１の制御部１５０は、コンテンツ素材１０１の無制限の再生を許すよう構成され、及び後続の詳細な処理は回避される。

【００３５】

２２０において、コンテンツ素材は受信され、又はコンテンツ素材の次のセグメントが受信され、セキュリティ情報が引き出される。

【００３６】

２３０において、例えば図１の評価器１２０に関し以上に詳細に説明されたようにセキュリティ試験／評価が実行され、そしてセキュリティスコアが決定される。図２のブロック２３０から破線により図示されたように、セキュリティ試験／評価は、継続的に繰り返

されて良い。ブロック２３０からのセキュリティスコアは継続的に、又はコンテンツ素材の最小セグメント数の受信及び試験のような特定の基準が満たされた後に提供されて良い。

【００３７】

２４０において、セキュリティ試験ブロック２３０の出力は、２１０において決定されたセキュリティ基準に対して評価される。この評価に基づき、２５０において、コンテンツ素材の復号／解読は制御される。この制御は、単なるオン／オフ制御、又は以下に更に詳細に議論されるような可変制御であって良い。

【００３８】

本発明の第２の態様によると、セキュリティ制御部１５０及び復号器１４０は、コンテンツ素材１０１の再生の際の品質／忠実度のレベルの変化を提供するよう構成される。この態様は、以上に議論された制御可能なセキュリティ基準１５１の使用と合わせて、又は独立して実施されて良い。

【００３９】

定量的スコア１２５はセキュリティ評価器１２０により提供されるので、セキュリティ制御部１５０は、復号器１４０の制御の程度の変化を提供するよう構成され得る。

【００４０】

本発明の態様の単純な実施例では、復号器１４０は、コンテンツ素材１０１の再生可能版の低次ビットを切り捨てるよう構成される。この実施例における切り捨ての程度は、セキュリティスコア１２５に基づきセキュリティ制御部１５０により決定される。選択的に、セキュリティ制御部１５０は、セキュリティ基準１５１に関連するセキュリティスコア１２５に基づき切り捨ての程度を決定する。

【００４１】

より複雑な実施例では、制御部１５０は、連続的復号器１４０でコンテンツ素材を復号するレベルを制御する。従来知られているように、いくつかの符号化方式は、階層的方法でコンテンツ素材１０１を符号化又は暗号化する。階層のトップレベルにおいて、素材の最も重要な特徴のみが符号化される。階層の後のレベルのそれぞれにおいて、細部の追加レベル又は解像度が符号化される。

【００４２】

図３は、連続的に符号化されたコンテンツの再生の品質レベルを動的に制御するセキュリティシステムの例であるフロー図を図示す。

【００４３】

３１０において、標準的にコンテンツ素材と関連付けられた「ヘッダー」情報から符号化レベルの数が決定される。３２０において、符号化レベルの数及び現在のコンテンツ素材のために決定されたセキュリティスコアに基づき、復号化レベルの数が決定され、選択的にはセキュリティ基準に基づき調整される。例えば、セキュリティ基準に関連する高セキュリティスコアは、結果として符号化レベル数と等しく設定されている復号化レベル数を生じる。他方で、セキュリティ基準と関連する低セキュリティスコアは、結果として符号化レベルより少ない復号化レベルを生じる。

【００４４】

ループ３３０－３５０は、３４０において、符号化レベルのそれぞれを、現在のコンテンツ素材と関連付けられたセキュリティスコアに基づき決定された復号化レベル数まで連続的に復号する。コンテンツ素材の再生の品質を制御することにより、コンテンツプロバイダー又は機器ベンダーは、許可コンテンツ素材のユーザーが、低い品質レベルにもかかわらず、疑わしい不正素材の再生を許すことにより、過度に制限されたセキュリティ規制のために経験する不満を低減し得る。

【００４５】

同様の方法で、コンテンツ素材と関連付けられたセキュリティの指標に基づく再生の品質を制御することにより、不正コピーの蔓延を低減し得る。例えば、コンテンツ素材の不正コピーが一般により低いセキュリティスコアを示すとすると、その結果生じるコピーの

それぞれは、最大品質より低い品質を有し、及びそれらの市場価値は低下させられる。

【００４６】

同様に、再生の品質は、再生の使用目的に基づき制御されて良い。つまり、例えば、復号化レベルの数の決定、又は切り捨てビットの数の決定は、素材のコピーを生成するために、又は素材の単なる再生のために再生が実行されているかどうかに依存して良い。

【００４７】

前述の記載は、本発明の原理を説明する。従って、当業者は、本発明の原理を実施し及び本発明の精神及び範囲に包含される、本願明細書に明示的に記載されない種々の構成を考案し得る。

【００４８】

これらの請求項を解釈する際、以下の点が理解されるべきである：

（ａ）「有する」の語は、与えられた請求項に列挙された以外の他の要素又は動作の存在を排除しない；

（ｂ）要素に先行する単数表記の語は、当該要素の複数の存在を排除しない；

（ｃ）請求項内の如何なる参照符号も当該請求項の範囲を制限しない；

（ｄ）複数の「手段」は、同一項目又はハードウェア又はソフトウェアで実施された構造又は機能により表現され得る；

（ｅ）開示された要素のそれぞれは、ハードウェア部分（例えば別個の及び統合された電子回路を有する）、ソフトウェア部分（例えばコンピュータープログラミング）、及びこれらの如何なる組み合わせも有して良い；

（ｆ）ハードウェア部分は、アナログ及びデジタル部分の１つ又は両方を有して良い；

（ｇ）これらの開示された装置又は部分の何れも、共に組み合わされるか、又は特に記載されない限り更なる部分に分離されて良い；

（ｈ）動作の如何なる特別なシーケンスも、特に支持されない限り必要とされない；

（ｉ）「複数の」要素の語は、請求された要素の２つ以上を有し、及び要素数の如何なる特定の範囲も示唆しない；つまり複数の要素はわずか２つの要素であり得る。

【図面の簡単な説明】

【００４９】

【図１】本発明によるセキュリティシステムの例であるブロック図を図示す。

【図２】本発明による保護コンテンツの再生を動的に制御するセキュリティシステムの例であるフロー図を図示す。

【図３】本発明による保護コンテンツの再生の品質レベルを動的に制御するセキュリティシステムの例であるフロー図を図示す。

【図１】

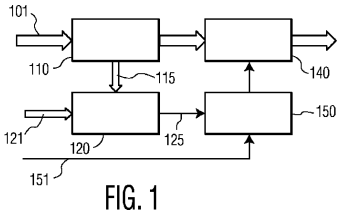

FIG. 1

【図２】

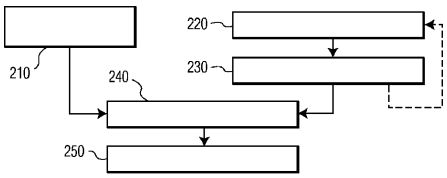

FIG. 2

【図３】

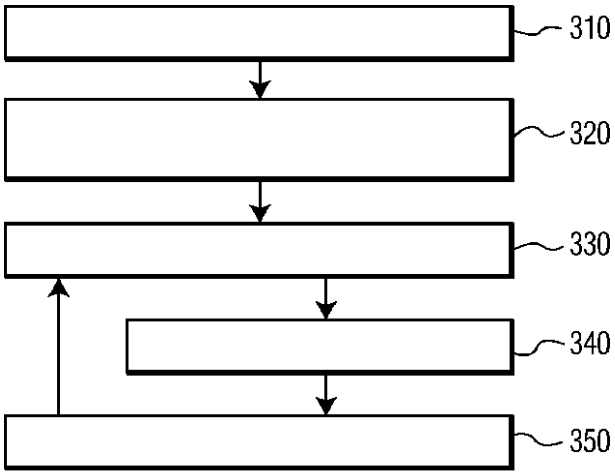

FIG. 3

フロントページの続き

(51)Int.Cl.			FI		
H04N	***7/167***	***(2011.01)***	H04N	7/167	Z
H04N	***7/173***	***(2011.01)***	H04N	7/173	610Z
			H04N	7/173	630

(72)発明者 バルビーリ，マウロ
オランダ国，5621 ベーアー アインドーフェン フルーネヴァウツウェッハ 1

審査官 戸島 弘詩

(56)参考文献 特開平11－073725（JP，A）
国際公開第01／031630（WO，A1）
特開平07－319691（JP，A）
特開2002－297555（JP，A）
特開平09－312039（JP，A）
国際公開第99／042996（WO，A1）
特表2004－534465（JP，A）
特表2004－503880（JP，A）
特表2004－532495（JP，A）
崔 潤基，誤り確率に基づく電子透かしの判定法と動画像透かしへの適用，電子情報通信学会論文誌，日本，社団法人電子情報通信学会，2002年 8月 1日，第J85-D-II巻，第8号，第1308頁

(58)調査した分野(Int.Cl.，DB名)
G06F21/00-21/24
G09C1/00-5/00
H04K1/00
H04L9/00
H04N5/91,7/10,7/14-7/173,7/20-7/22
G11B20/10
G06T1/00
H04N1/38