(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2009-501470
(P2009-501470A)
(43)公表日　平成21年1月15日(2009.1.15)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/14	(2006.01)	H04L	9/00	641	5J104
G06Q 50/00	(2006.01)	G06F	17/60	142	
G06Q 30/00	(2006.01)	G06F	17/60	302E	

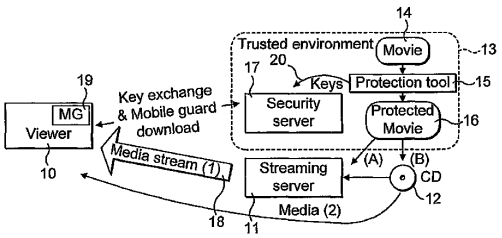
審査請求 未請求　予備審査請求 有　（全 35 頁）

(21)出願番号　特願2008-520958 (P2008-520958)
(86)(22)出願日　平成18年7月14日 (2006.7.14)
(85)翻訳文提出日　平成20年3月4日 (2008.3.4)
(86)国際出願番号　PCT/GB2006/002619
(87)国際公開番号　WO2007/007112
(87)国際公開日　平成19年1月18日 (2007.1.18)
(31)優先権主張番号　0514492.8
(32)優先日　平成17年7月14日 (2005.7.14)
(33)優先権主張国　英国 (GB)

(71)出願人　508011979
セクストリーム　テクノロジーズ　エーエス
Ｓｅｃｕｓｔｒｅａｍ　Ｔｅｃｈｎｏｌｏｇｉｅｓ　ＡＳ
ノルウェー王国、７０１３　トロンハイム、キョプマンスガタ　５
Ｋｊｏｅｐｍａｎｎｓｇａｔａ　５，　７０１３　Ｔｒｏｎｄｈｅｉｍ，　Ｎｏｒｗａｙ
(74)代理人　100083116
弁理士　松浦　憲三
(72)発明者　ギスル　グリメン
ノルウェー王国、７０５２　トロンハイム、　ティホルト　アレ　１４ａ
最終頁に続く

(54)【発明の名称】マルチメディア・データの保護

(57)【要約】
本発明は、（ａ）ドキュメントのそれぞれの時間的に区切られたセグメントに対応する一連の異なるキーを使用して著作物を暗号化するステップと、（ｂ）クライアントの状態の関数である結果を有するアルゴリズムを含むソフトウェア・コードをセキュリティ・サーバからクライアントに送信するステップと、（ｃ）クライアントにおいてコードを実行し、結果をセキュリティ・サーバに返すステップと、（ｄ）結果が未修正のクライアントを示すかどうかを判定するステップとを含み、（ｅ）セグメントをサーバからクライアントに送信するステップと、（ｆ）送信されたセグメントに対応するキーを安全なリモート・サーバからクライアントに安全にストリーミングするステップと、（ｇ）取得されたメディア・キーを使用してセグメントを復号化するステップと、（ｈ）ステップ（ｄ）が修正されたクライアントを示す場合にさらなるキーが送信されることを防止し、ステップ（ｄ）が修正されたクライアントを示さない場合にステップ（ｅ）から（ｇ）までを繰り返し、ステップ（ｂ）から（ｄ）までを繰り返すステップとをさらに含む、映画



【特許請求の範囲】
【請求項１】
メディア著作物をクライアントに送信する方法であって、
（ａ）前記著作物のそれぞれの時間的に区切られたセグメントに対応する一連の異なるキーを使用して前記著作物を暗号化するステップと、
（ｂ）第１のキーを安全なサーバから前記クライアントに安全に送信し、対応するセグメントをサーバから前記クライアントに送信するステップと、
（ｃ）前記クライアントにおいて、前記対応するセグメントを復号化するために前記第１のキーを使用するステップと、
（ｄ）ビューアにおいて、復号化された部分を表示するステップと、
（ｆ）さらなるセグメント及びキーについてステップ（ｂ）から（ｄ）までを繰り返すステップと
を含む、方法。
【請求項２】
前記キーが、いかなるキーも２つ以上のセグメントを復号化するために使用することができないように暗号として互いに独立している、請求項１に記載の方法。
【請求項３】
前記クライアントが前記ドキュメントを受信する権利を与えられていることのチェックの後でのみキーが供給される、請求項１又は２に記載の方法。
【請求項４】
前記キーが、前記安全なサーバと前記クライアントの間の協力を強制するために使用される、請求項１、２又は３に記載の方法。
【請求項５】
各キーが所定の長さのセグメントに対応する、請求項に記載の方法。
【請求項６】
前記安全なサーバが前記クライアントから離れている、前記請求項のいずれかに記載の方法。
【請求項７】
前記キーが、ランダム・データ・ジェネレータと、前記クライアントに知られている前記安全なサーバの公開キーとを使用するキー交換プロトコルを使用して送信される、前記請求項のいずれかに記載の方法。
【請求項８】
各キーが前記クライアントによって個々に要求されなければならない、前記請求項のいずれかに記載の方法。
【請求項９】
前記クライアントが不正に変更されていないことを保証するために前記クライアントのインテグリティをチェックするステップをさらに含む、前記請求項のいずれかに記載の方法。
【請求項１０】
前記セキュリティ・サーバが、クライアントの修正が検出される場合、及び／又は前記クライアントのインテグリティ・チェックが成功でない場合にキーの供給を停止するように構成される、請求項９に記載の方法。
【請求項１１】
前記クライアントの前記インテグリティが（明細書において定義される）モバイル・ガードによってチェックされる、請求項９又は１０に記載の方法。
【請求項１２】
前記各キーが、前記クライアントの前記インテグリティを成功裏に検証したモバイル・ガードの信頼できる間隔の間にのみ送信される、請求項１１に記載の方法。
【請求項１３】
前記クライアントが修正されていない場合にのみ正しい結果を返すランダムに生成され

るアルゴリズムの使用を含む、請求項９、１０又は１１に記載の方法。
【請求項１４】
たとえキーの前記供給が停止されたとしても送信が継続することができるように前記セグメントが前記対応するキーとは独立に送信される、前記請求項のいずれかに記載の方法。
【請求項１５】
前記メディア著作物が記録物である、前記請求項のいずれかに記載の方法。
【請求項１６】
前記メディア著作物がライブ・パフォーマンスである請求項１乃至１４のいずれかに記載の方法。
【請求項１７】
前記メディア著作物がリモート・サーバから前記クライアントにストリーミングされる、前記請求項のいずれかに記載の方法。
【請求項１８】
データをクライアントに送信する方法であって、
（ａ）前記データを前記クライアントに送信するステップと、
（ｂ）前記クライアントの状態の関数である結果を有するアルゴリズムを含むソフトウェア・コードをセキュリティ・サーバから前記クライアントに送信するステップと、
（ｃ）前記クライアントにおいて前記コードを実行し、結果を前記セキュリティ・サーバに返すステップと、
（ｄ）前記結果が未修正のビューアを示すかどうかを判定するステップと
を含む、方法。
【請求項１９】
前記データがメディア著作物である、請求項１８に記載の方法。
【請求項２０】
ステップ（ｄ）が実行されるまで前記クライアントが前記データを使用することが防止される、請求項１８又は１９に記載の方法。
【請求項２１】
前記結果が未修正のビューアを示さない場合に前記データの及び／又は前記データを復号化するために必要なキーの送信を停止するステップ（ｅ）をさらに含む、請求項１８、１９又は２０に記載の方法。
【請求項２２】
前記コードが、前記クライアントのプログラム・コード及び／又はメモリ・イメージが入力されるチェックサムの計算を含む、請求項１８乃至２１のいずれかに記載の方法。
【請求項２３】
前記チェックサムの計算は前記チェックサムの計算の入力に乱数を含む、請求項２２に記載の方法。
【請求項２４】
前記クライアントは前記乱数を前記セキュリティ・サーバの公開キーを用いて暗号化し、前記暗号化された乱数はメディア・キーの要求及び計算されたチェックサムと共に前記セキュリティ・サーバに送信され、前記セキュリティ・サーバは前記乱数を復号化し、前記復号化された乱数を使用して前記メディア・キーを暗号化し、前記セキュリティ・サーバは前記乱数を使用して前記セキュリティ・サーバ自身の前記チェックサムの計算を更新し、続いて前記セキュリティ・サーバは前記チェックサムの２つの値を比較する、請求項２３に記載の方法。
【請求項２５】
前記２つの値が等しい場合かつその場合に限り、前記暗号化されたメディア・キーが前記クライアントに送信され、その結果、前記クライアントは前記メディア・キーを復号化することができる、請求項２４に記載の方法。
【請求項２６】

前記２つの値が等しくない場合に、前記クライアント・ビューアが不正に変更されたと判定される、請求項２５に記載の方法。

【請求項２７】

前記コードが前記ビューア上で（１つ又は複数の）難読化タスクを実行する、請求項１８乃至２６のいずれかに記載の方法。

【請求項２８】

前記（１つ又は複数の）難読化タスクが、実行中のビューアのメモリ・イメージをランダム化することを含む、請求項２７に記載の方法。

【請求項２９】

前記難読化タスクが以下のこと、すなわち、全て明細書において定義される、コード再配置、コード多様化、コード再配置、及びデータ隠蔽のうちの１つ又は複数を含む、請求項２７に記載の方法。

【請求項３０】

前記モバイル・ガードが難読化される、請求項１８乃至２９のいずれかに記載の方法。

【請求項３１】

実行中のビューアを難読化する方法であって、前記実行中のビューアのメモリ・イメージをランダム化することを含む、方法。

【請求項３２】

メディア著作物をクライアントに送信する方法であって、

（ａ）前記著作物のそれぞれの時間的に区切られたセグメントに対応する一連の異なるキーを使用して前記著作物を暗号化するステップと、

（ｂ）前記クライアントの状態の関数である結果を有するアルゴリズムを含むソフトウェア・コードをセキュリティ・サーバから前記クライアントに送信するステップと、

（ｃ）前記クライアントにおいて前記コードを実行し、結果を前記セキュリティ・サーバに返すステップと、

（ｄ）前記結果が未修正のクライアントを示すかどうかを判定するステップと、

（ｅ）セグメントをサーバから前記クライアントに送信するステップと、

（ｆ）前記結果が未修正のクライアントを示す場合に、前記送信されたセグメントに対応するキーを安全なリモート・サーバから前記クライアントに安全にストリーミングするステップと、

（ｇ）前記キーを使用して前記セグメントを復号化するステップと

を含む、方法。

【請求項３３】

それぞれのアルゴリズムを含むソフトウェア・コードが関連する信頼できる間隔を有し、前記信頼できる間隔の間に複数のキーが前記クライアントにストリーミングされる、請求項３２に記載の方法。

【請求項３４】

ステップ（ｂ）から（ｇ）までが繰り返されるさらなるステップ（ｈ）をさらに含む、請求項３２又は３３に記載の方法。

【請求項３５】

メディア著作物をクライアントに送信する方法であって、

（ａ）ドキュメントのそれぞれの時間的に区切られたセグメントに対応する一連の異なるキーを使用して前記著作物を暗号化するステップと、

（ｂ）前記クライアントの状態の関数である結果を有するアルゴリズムを含むソフトウェア・コードをセキュリティ・サーバから前記クライアントに送信するステップと、

（ｃ）前記クライアントにおいて前記コードを実行し、結果を前記セキュリティ・サーバに返すステップと、

（ｄ）前記結果が未修正のクライアントを示すかどうかを判定するステップと

を含み、

（ｅ）セグメントをサーバから前記クライアントに送信するステップと、

（ｆ）前記送信されたセグメントに対応するキーを安全なリモート・サーバから前記クライアントに安全にストリーミングするステップと、
（ｇ）前記取得されたメディア・キーを使用して前記セグメントを復号化するステップと、
（ｈ）ステップ（ｄ）が修正されたクライアントを示す場合にさらなるキーが送信されることを防止し、ステップ（ｄ）が修正されたクライアントを示さない場合にステップ（ｅ）から（ｇ）までを繰り返すステップと
をさらに含む、方法。
【請求項３６】
ステップ（ｂ）から（ｄ）までを繰り返すステップ（ｉ）をさらに含む、請求項３５に記載の方法。
【請求項３７】
クライアント・プログラムの状態に依存するアルゴリズムを含むソフトウェア・コードを安全なソースから、前記クライアント・プログラムを実行するクライアント・コンピュータに送信するステップと、前記ソフトウェア・コードを実行するステップと、それによって前記ソースが前記クライアント・プログラムのインテグリティを判定することができる結果を前記ソースに返すステップとを含む、クライアント・プログラムのインテグリティをチェックする方法。
【請求項３８】
前記クライアント・プログラムが以下のこと、すなわち、インターネット・バンキング、オンライン・ゲーム、及び分散計算のうちの１つにおいて使用される、請求項３７に記載の方法。
【請求項３９】
前記請求項のいずれかに記載の方法に従って動作するように構成された装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、映画、ＴＶ番組、オーディオ・ドキュメントなどの時間次元を有するマルチメディア著作物の安全な配布に関する。具体的には、本発明は、ユーザが著作物の不正コピーを取得することを防止するやり方でそのような著作物をユーザに安全に配布するためのシステムに関する。
【背景技術】
【０００２】
本発明の態様は、オンライン・バンキング、ゲームなどのその他のサーバ・クライアントの状況にも応用できる。
【０００３】
芸術作品の不正コピーは絶え間のない問題である。映画産業の黎明期において、映画の不正コピーが作成されることは可能であったが、不正コピーを作成することは高価であり、専門の機材を使用できる人を除いて実行不可能であった。ホーム・ビデオ・レコーダの登場と共に、映画及びその他の記録されたプログラムに関する新しい市場が制作者に利用可能になったが、同時に、それらの記録物が不正にコピー及び配布されることが可能になった。
【０００４】
今日、より高品質の再生及びより便利でコンパクトなデータ持ち運び手段を提供するＤＶＤフォーマットが急速にビデオに取って代わりつつある。さらに、手頃なブロードバンド・インターネット接続の登場によって、映画及びその他のメディアをリモート・サーバからホーム・コンピュータ上にダウンロード又はストリーミングすることに関する市場が現在現れつつある。
【０００５】
メディア著作物がダウンロードされる場合、そのメディア著作物のコピーがコンピュー

タのハード・ドライブ上に記憶され、ビデオ記録を見るのと同様に、通常はそのコピーはユーザによって繰り返し見られることができる。ライブであろうと録画であろうと、ストリーミング・コンテンツは、（従来のＴＶ番組と同様に）そのストリーミングがコンピュータに送信されるときにほぼリアルタイムで（いくらかのバッファリングを提供する必要があるので短い遅延がある）視聴される。ラジオ及び一部のＴＶ局がそれらの局のコンテンツをこのやり方で提供することがよく知られている。

【０００６】

これらの技術の向上はメディア企業に対して有望な新しい市場の発展を可能にしたが、著作物の不正コピーの作成及び配布を防止する対応する問題も存在する。低価格のホーム・コンピュータでさえもコンテンツをＤＶＤ上に記録する機能を有することが今や当たり前である。

【０００７】

したがって、そのようなコピーを防止する目的で技術が開発されてきた。従来のアプローチにおいて、ここでは「コンテンツ・プロバイダ」と呼ばれるメディア供給者が、概して「メディア著作物」と呼ばれることになる符号化されたメディア著作物、例えば映画を所有する。これらは、符号化されたメディア著作物のコピーをユーザが作成することを許さないやり方でユーザのクライアント・プログラム／ビューアに配布及び表示されるべきである。配信は、ネットワーク上のストリーミングによって、又はユーザに物理メディア、例えばＤＶＤを届けることによってのいずれかで実行されることができる。

【０００８】

著作物がネットワーク上で伝達される場合、通常、それは、当該著作物を第三者に傍受及び複製されることから守るための暗号化手段によって保護される。我々は、これらの暗号化手段を「伝達暗号化」と呼ぶ。（セキュリティ対策である暗号化は、それによって容易に及び効率的に送信されることができる形態に著作物が変換され、通常は圧縮される符号化とは区別されるべきである。）暗号化技術は十分に発達しており、コンピュータ・ネットワーク上の通信が適切なやり方で保護されることができることを保証する。

【０００９】

メディア著作物がクライアントに配信される前に、コンテンツの所有者は符号化されたメディア・ドキュメントを暗号化手段を使用して保護する。安全な「プロバイダ環境」内で「メディア・キー」を用いて著作物を暗号化して暗号化された符号化メディア著作物、「暗号化著作物」を作成するために暗号化ツールが使用される。

【００１０】

この意図は、クライアントが著作物を復号化することを可能にするメディア・キーをクライアントが持っている場合にのみクライアントが当該著作物を使用することができることである。これは、クライアント・プログラム／ビューア／プレイヤ及び／又はメディア内、例えばＤＶＤプレイヤ及びＤＶＤ内に組み込まれることができる（クライアント・プログラム／ビューア／プレイヤは、独立したデバイスであるか、又はコンピュータ上のビューア・ソフトウェア・プログラムであってよい。）。

【００１１】

図１に概略的に示される別のオプションは、メディア・キーがライセンス・サーバ１からオン・デマンドで取得されることである。これは、メディア著作物のストリーミングを可能にする。このモデルをサポートするために、暗号化ツール２が追加的な情報と一緒にメディア・キーをライセンス３にラップし、これをライセンス・サーバ１に送信する。次に、クライアントは、暗号化された符号化メディア・ストリーム４がクライアントに対して表示されることができる前にビューア６において復号化される必要がある暗号化された符号化メディア・ストリーム４をストリーミング・サーバ５から受信する。暗号化された映画７を視聴するために、ビューアは、ライセンス・サーバからメディア・キーを含むライセンスを要求する（図１の「開始フェーズ」参照）。

【００１２】

いったんビューアがライセンス３（及び、ひいてはメディア・キー）を受信してしまう

と、ビューアは、そのストリーミング・サーバ５からそのビューアが暗号化された符号化メディア・ストリーム４を受信するストリーミング・サーバ５に接続する。ビューアはメディア・キーを使用して、暗号化された符号化メディア・ストリームを復号化し、そのメディア・ストリームをクライアントに対して表示する（図１の「ストリーミング・フェーズ」参照）。

【００１３】

上述のシナリオにおける主な問題は、クライアントによって制御されるホスト上でビューアが実行されることである。したがって、ビューアは、（映画９が最初に暗号化された）信頼できる環境８内で実行されない。したがって、クライアントがビューアを修正する恐れがあるリスクが存在する。たとえビューアが通常はメディア・ストリームの一部を復号化及びデコードするだけであるとしても、表示プロセス全体の間に、符号化メディア・ストリームのあらゆる部分がある時点でビューアのメモリ・イメージ内に存在することになる。別のリスクは、ビューアのメモリ・イメージがキーを含む必要があるので、ユーザがメディア・キーを抽出する恐れがあり、その場合、ユーザが暗号化されていない符号化メディアのコピーを作成することができることである。

【００１４】

修正の問題は、純粋なソフトウェア・ベースのビューアに対しても、ハードウェア・ベースのビューア、例えば、指定されたＤＶＤプレイヤに対しても存在する。ハードウェア・ベースのビューアを修正することはソフトウェア・ベースのビューアを修正することよりも難しいが、それは不可能ではない。

【発明の開示】

【発明が解決しようとする課題】

【００１５】

したがって、これらの欠点に対処するシステムに対するニーズが存在する。

【００１６】

任意の効果的な保護メカニズムに対する全般的な要件は以下のことを含む。保護メカニズムは、破るコストが著作物の価値と少なくとも同じ大きさであるように破るために資源を多量に必要としなければならない。任意の成功する攻撃が、その攻撃が別の所に適用されることができるように一般化可能であってはならない。また、好ましくは、保護メカニズムは検出を容易にすべきである。

【課題を解決するための手段】

【００１７】

以下で説明される本発明の種々の態様はこれらの要件に個々に対処し、本発明の好ましい形態はそれらの要件全てを満足するシステムを提供する。

【００１８】

以下の検討において、メディア著作物は時間的側面を有する著作物である、すなわち、メディア著作物は適切な順序で実行される必要があるいくつかの表示ステップを含む。通常、これらのステップは計算上互いに独立しており、個々に処理されることができる。ほとんどの場合、完全な表示は多大な量の時間、すなわち、映画の場合には何分も、又は何時間も要する。

【００１９】

本発明の一態様によれば、

（ａ）著作物のそれぞれの時間的に区切られたセグメントに対応する一連の異なるキーを使用して著作物を暗号化するステップと、

（ｂ）第１のキーを安全なサーバからクライアントに安全に送信し、対応するセグメントをサーバからクライアントに送信するステップと、

（ｃ）クライアントにおいて、対応するセグメントを復号化するために第１のキーを使用するステップと、

（ｄ）ビューアにおいて、復号化された部分を表示するステップと、

（ｅ）さらなるセグメント及びキーについてステップ（ｂ）から（ｄ）までを繰り返す

ステップと
を含む、メディア著作物をクライアントに送信する方法が提供される。
【００２０】
本発明は、（上述のように）時間的側面を有する任意の種類のメディア著作物に適用可能であり、映画を配布すること、例えばそれらの映画をインターネット上でストリーミングすることに特に有用である。
【００２１】
ドキュメントを一連のセグメントに分割することによって、各キーが１つのセグメントだけを復号化可能であり、すなわちキーが機能的に独立しているので小部分を超えてコピーすることは実行不可能になる。したがって、映画の１つのセグメントだけが一度にコピーされることができる。さらに、その他のキーを解除することができるマスタ・キーは存在すべきでなく、すなわち、好ましくはキーは構造的に独立しているべきである。例えばほんの数秒、例えば２秒又は３秒以下、及び最も好ましくは１秒以下の所定の長さのセグメントにそれぞれのキーが対応するように、映画の典型的な長さに対して数千の異なるキーが使用されることが好ましい。ほとんどの種類のメディア著作物は、それらのメディア著作物が実質的に完全である場合にのみ大きな価値を持つ。例えば、最後の数分のみがない映画は、通常はわずかな価値しかない。したがって、映画を不正にコピーしようとする者は、セグメントのそれぞれを復号化する必要がある。
【００２２】
データの復号化の連続的なフローを維持するために、いくつかの実施形態において、クライアントは現在のキー及び（１つ又は複数の）次のキーを要求し、少数のキー（例えば、２個、３個、４個程度）をメモリ内にキャッシュする可能性がある。
【００２３】
通常、安全なサーバはビューアから離れており、本明細書においては「セキュリティ・サーバ」と呼ばれる。
【００２４】
概して、映画は信頼できる環境内で暗号化される。好ましくは、暗号化中に生成されたキーは、信頼できるプロバイダ環境内にあるセキュリティ・サーバに供給される。しかし、次にキーがセキュリティ・サーバからビューアに送信されるが、映画又はその他の著作物は他の所から送信されてもよい。例えば、映画またその他の著作物は、信頼できる環境の外にある別個のサーバからストリーミングされてよい。したがって、１つの好ましい実施形態において、信頼できるプロバイダ環境内で映画がいったん暗号化されてしまうと、次にその映画は安全でないストリーミング・サーバに供給される。
【００２５】
したがって、この構成において、リモート・コンピュータ（例えば、ユーザのＰＣ）上で実行されるソフトウェア・ビューア・プログラムであってよいクライアントは、（メディア・キーと呼ばれる）キーを受信するためにセキュリティ・サーバと通信し、別個のストリーミング・サーバと通信する。
【００２６】
メディア・キーはクライアントからの要求の後でクライアントに送信されることが好ましく、これは、ランダム・データ・ジェネレータと、ビューアに知られているセキュリティ・サーバの公開キーとを使用するキー交換プロトコルを使用して行われることが好ましい。
【００２７】
１つの実装において、次のメディア・キーを取得することが必要なとき、クライアントはランダム・データを生成し、そのデータをセキュリティ・サーバの公開キーを用いて暗号化する。次に、暗号化されたデータは、セキュリティ・サーバに送信される、好ましくは当該クライアントを特定するデータを伴う次のメディア・キーの要求に含められることができる。セキュリティ・サーバが要求を受信するとき、セキュリティ・サーバは、そのクライアントがメディア著作物を受信する権利があるかどうかをチェックし、ランダム・

データを復号化及び抽出し、そのランダム・データと要求されたキーとを使用する関数を実行して、ランダム・データを使用して当該キーを暗号化する。一実施形態において、それらはＸＯＲ演算されることができる。次に、結果がクライアントに返信される。クライアントが結果を受信するとき、次にクライアントは、例えば、当該結果を最初のキーの要求において提供された同じランダム・データとＸＯＲ演算することによって対応する関数を実行することによって当該結果から要求されたキーを抽出することができる。このようにして、ビューアのソース・コード内に隠蔽されたいかなる秘密キーもなしに、暗号化された符号化メディア・ストリームが復号化されることができる。

【００２８】

公開鍵が交換される「中間者」攻撃を防ぐために公開キーがチェックサムの計算に含められることが好ましい。

【００２９】

プロトコルの好ましい形態において、モバイル・ガードによってチェックされるクライアントが、ランダム・データを生成するクライアントと同じクライアントであることを保証するためのステップも行われる。これは、メディア・キーを要求するために使用されるランダム・データを含むようにチェックサムに対する入力を拡大することによって行われることができる。したがって、チェックサムに対する入力は、クライアントからのコードと、セキュリティ・サーバの公開キーと、キーの要求と共に送信されるランダム・データとを含むことができる。

【００３０】

外部エントロピー・ソースは監視され得るので、乱数の生成のために使用されるエントロピー・ソースは、タスクがどのようにスケジューリングされ、中断されるかの形態で実行環境自体によって生成されるエントロピー・ソースである可能性がある。したがって、ランダム生成プロセスは、ビューア及び実行中のモバイル・ガードの現在の状態からのデータと共に安全なハッシュ・アルゴリズムに入力されることができる様々な計算タスクに従事するいくつかのスレッドを作成することで構成される可能性がある。

【００３１】

連続する一連のキーがクライアントによって受信されることの要求が、ユーザの協力を強制するために使用されることができる。したがって、プロバイダによって要求される特定のステップがクライアントによって実行されないとき、キーの供給が停止されることができる。以下でさらに検討されるように、このステップはクライアントのインテグリティ・チェックであることができ、好ましくは、新しいキーの要求はいわゆる「モバイル・ガード」がビューアが修正されていないことを示すときにのみ応じられる。

【００３２】

モバイル・ガードが使用される場合、実際のクライアント・ビューア／プレイヤ・プログラムではなくそのモバイル・ガードが上述の好ましいキー交換プロトコルにおいて使用される乱数を生成することが可能である。

【００３３】

コンテンツ・プロバイダがメディア著作物を制御するのでこの協力の強制が可能なのであり、著作物の時間的性質のおかげで、後続の部分を受信するために協力するようにユーザが要求されるようにして著作物が小部分の形で供給されることができることが理解されるであろう。これは、ライセンスがドキュメント全体を解除し、事実上、時間的性質を無駄にする従来のシステムと対称的である。

【００３４】

本発明の代替実施形態において、信頼できる環境がストリーミング・サーバがその環境に含まれるように拡大される。この拡大が行われるとき、ストリーミング・サーバにメディア・キーを生成させ、メディア・ストリームをオン・ザ・フライで暗号化させることが可能である。これは、各メディア・ストリームがメディア・キーの一意的な組によって暗号化されることを保証する。そのことは、漏洩したメディア・キーが同じ映画の異なるコピーを復号化するために使用されることができないことを意味する。メディア・キーの配

布を容易にするためにストリーミング・サーバがそれらのメディア・キーをセキュリティ・サーバに送信し、それらのセキュリティ・サーバが上述のようにそれらのメディア・キーをビューアに配布することになる。欠点は、別のエンティティが信頼できる必要があること、及びオン・ザ・フライの暗号化は計算コストが高いことである。したがって、ここで、一方の非常に高いセキュリティと、他方の信頼できる環境の複雑性及び計算コストとの間のトレード・オフが存在する。

【００３５】

本発明は、ドキュメントがリモート・サーバからストリーミングされる構成に限定されない。ドキュメントが暗号化されるので、ドキュメントは、任意の都合のよいやり方で配布されることができる。したがって、暗号化されたドキュメントはローカル・サーバからクライアントに、又は物理メディア（例えば、ＤＶＤ）上に提供されることができる。そのとき、ドキュメントはローカル・サーバ又は物理メディアからビューアに送信され、上述されたのと同じやり方で復号化されることができる。

【００３６】

この構成は従来技術のシステムに優る著しい改善を提供するが、ビューアが不正に変更される可能性があり、その結果、復号化された著作物（映画など）が記録及びコピーされる可能性があるリスクがまだ残る。したがって、本発明はビューアが不正に変更されていないことを保証するためにビューアのインテグリティをチェックするための手段をさらに含むことが好ましい。これは、規則的な間隔で、及び／又はキーが要求されるときにチェックサムなどの信号をセキュリティ・サーバに送信するようにそれをプログラムすることによって行われることができる。そのような信号は、ビューアに対するあらゆる修正が信号を変更するようにビューアの状態によって決まるように設計される。

【００３７】

しかし、そのような対策は修正されたビューアをそのビューアの本当の状態によらずに「正しい」信号を送信するようにプログラムすることによってくぐり抜けられる可能性があるというリスクがある。したがって、方法は、時間と共に変化するいくつかの異なる試験を使用してセキュリティ・サーバがビューアを取り調べることをさらに要求することが好ましい。特に好ましい形態において、試験は、ビューアが修正されていない場合にのみ正しい結果を返すランダムに生成されるアルゴリズムの使用を含む。さらに、応答の失敗、又は応答における過度の遅延は、ビューアの修正の指示と考えられることができる。

【００３８】

したがって、セキュリティ・サーバは、ビューアの修正が検出される場合、及び／又はそのようなビューアのインテグリティ・チェックが成功でない場合にキーの供給を停止するように構成されることが好ましい。

【００３９】

最も好ましい構成は、アルゴリズムがセキュリティ・サーバによってクライアントにソフトウェア・コード（例えば、マシン・コード）の形態で送信されることである。このソフトウェア・コードは「モバイル・ガード」と呼ばれる場合があり、本明細書においてさらに説明される。

【００４０】

インテグリティをチェックするそのようなシステムはそれ自体で発明概念と見なされ、したがって、さらなる態様から見て、

（ａ）データをクライアントに送信するステップと、

（ｂ）クライアントの状態の関数である結果を有するアルゴリズムを含むソフトウェア・コードをセキュリティ・サーバからクライアントに送信するステップと、

（ｃ）クライアントにおいて当該コードを実行するステップと、

（ｄ）結果をセキュリティ・サーバに返すステップと、

（ｅ）結果が未修正のビューアを示すかどうかを判定するステップと

を含む、データをクライアントに送信する方法が提供される。

【００４１】

データは、例えばインターネット上でクライアントにストリーミングされるメディア著作物であることができるか、又はデータは、上述のようにローカル・サーバ、ＤＶＤ、又はその他のメディアから供給されることができる。しかし、以下でより十分に検討されるように、データは、サーバとクライアントの間で送信されることができる任意の種類のデータであってよい。クライアントはコンピュータ上で実行されるプログラムか、又はＴＶセット・トップ・ボックスなどのハードウェア・デバイスであってよい。ステップ（ｂ）において参照されるアルゴリズムがドキュメントの任意の部分が送信される前に送信されることができるか、又は著作物の全てもしくは一部がアルゴリズムの前に送信されることができる。ドキュメントはステップ（ｄ）が実行されるまで見られないことが好ましい。

【００４２】

ステップ（ｄ）における結果に応じて適切な対応が取られることができる。著作物がストリーミングされている場合、ビューアが修正されていないことが分かったとすると、通常、著作物の及びその著作物を復号化するために必要とされる任意のキーの送信は継続することが許される。しかし、結果が未修正のクライアントを示さない場合に著作物の及び／又はその著作物を復号化するために必要なキーの送信を停止するさらなるステップ（ｅ）が存在することができる。モバイル・ガードから結果が返されない場合、これもクライアントが修正されたことを示すと見なされることが好ましい。

【００４３】

著作物がローカル・サーバ、ＤＶＤなどのローカル・ソースから送信されている場合、対応は、ドキュメントを復号化するために必要とされるキーの送信を停止することであってよい。

【００４４】

代替として、クライアントが修正されたことが発見される場合にその他の対応が取られてよい。例えば、送信は継続することを許される可能性があり、ユーザを特定するために証拠が集められる可能性がある。これは、例えば、犯罪活動を検出するために、又はドキュメントの将来の違法コピーを防ぐために法的な又は調査的な対応を取ることが望ましい場合に適切である可能性がある。

【００４５】

上述のように、修正されたクライアントの特定に応答して取られる対応は、復号化のキーの送信を停止することであってよい。したがって、方法は、著作物を異なるキーを使用して暗号化される複数の時間的に区切られたセグメントに分割することをさらに含むことができることが理解されるであろう。これらのキーは、連続的に、及び好ましくは上述のようにクライアントに配布されることができる。したがって、それらのキーの配布が停止されるとき、著作物の残りの部分は復号化されることができない。

【００４６】

方法は、（上述のように）ソフトウェア・コード内のランダムに生成された秘密のアルゴリズムを使用して実行されることが好ましい。これらのいわゆる執行アルゴリズムは、クライアントの（例えば、ビューア・プログラムの）状態によって決まる結果を生成するが、ランダムな性質のおかげで正しい結果がユーザによって推測されることはできない。好ましくは、それらの執行アルゴリズムは、ビューア・プログラムのコードが入力されるチェックサムの計算を含む。アルゴリズムは全体として秘密であるが、チェックサムの計算は、ランダム化された入力の修正と組み合わせて使用されることができるＭｅｓｓａｇｅ　Ｄｉｇｅｓｔ　Ａｌｇｏｒｉｔｈｍ　５（ＭＤ５）（ＲＦＣ１３２１　ｗｗｗ．ｆａｑｓ．ｏｒｇ／ｒｆｃｓ／ｒｆｃ１３２１．ｈｔｍｌ）などの知られているチェックサムの計算であってよい。

【００４７】

入力の修正は、チェックサムに入力されることになるデータを並べ替えるモディファイアのランダムな生成を指す。１つの実装において、（ここでは「モバイル・ガード」と呼ばれる）ソフトウェア・コードが生成されるときにランダムな順序が決定される。アルゴリズムが実行されるとき、ビューアからの入力コードが同じサイズのｎ個のブロックに分

割される。次に、これらのブロックは上述のランダムな順序にシャッフルされ、それから、結果がチェックサム・アルゴリズムに入力される。この構成においてはチェックサム・アルゴリズム自体は公開されているが、そのアルゴリズムの結果はｎ個のブロックがそのアルゴリズムに入力される順序の関数である。この順序はセキュリティ・サーバに知られており、したがって、セキュリティ・サーバはそのセキュリティ・サーバに返された結果が元のままのビューアを示すかどうかを判定することができる。

【００４８】

入力がフィルタリングされるチェックサムを生成することに対する代替的なアプローチは、知られているチェックサム・アルゴリズムを分解し、入力を所与の順序で読むやり方でそれを再組立することである。

【００４９】

入力のフィルタリングを使用する代わりに、一からチェックサム関数を生成することが可能である。したがって、入力はｌワード（３２ビット）に分割されることができ、入力からのｌワードと、ワードを出力する変数領域からのｍワードとを読む関数ｆが生成される。関数は、逐次的に実行されるランダムな回数の割り当てを含むことができ、チェックサムはｆの適用の全ての結果の合計のモジュロ2^{32}であることができる。

【００５０】

関数を構成することは、チェックサム・アルゴリズムのほぼ全てのコードがランダムに生成され、コードにおけるより大きな構造的多様性をもたらすという利点を有する。ビルディング・ブロックが非常に小さいので、それはその他のアルゴリズムとのより容易なインターリーブを可能にする。

【００５１】

ソフトウェア・コードは、秘密であるか又は秘密でなくてよい追加的なアルゴリズムも含むことが好ましい。それらのアルゴリズムは、機能的に及び／又は空間的に秘密のアルゴリズムと関わり合わされることが好ましい。このように、クライアントのコンピュータ／ビューアが追加的なアルゴリズムを実行しない場合は秘密のアルゴリズムが実行されないので、クライアントのコンピュータ／ビューアは追加的なアルゴリズムを実行するように強制されることができる。追加的なアルゴリズムは、例えばビューアのハードウェアのインテグリティをチェックするために使用されることができる。

【００５２】

モバイル・ガードがビューアと同じ環境に存在するので、モバイル・ガードは潜在的に攻撃を受けやすい。ユーザは、そのモバイル・ガードが実行する保護方法をくぐり抜けるためにそのモバイル・ガードを修正しようと試みる可能性がある。モバイル・ガードに対する自動化された攻撃は、モバイル・ガードが上述のように部分的にランダムに生成されることを保証することによって防止されることができる。さらに、難読化変換がモバイル・ガードに適用されることができる。モバイル・ガードは、当該モバイル・ガードに固有のやり方でチェックサムとインターリーブされる不透過なデータ構造内にチェックサムを隠蔽することができる。変数はモバイル・ガードのメモリ内にランダムに配置されることができ、さらにモバイル・ガードの命令はメモリ内にやはりランダムに配置されるブロックに分割されることができる。これは、エントリ・ポイントをモバイル・ガード内に含めることが好ましい。実際、１つのモバイル・ガードに対するエントリ・ポイントは、前のモバイル・ガードによって提供されることができる。

【００５３】

これらのステップが実行される場合、任意の自動化された攻撃が始まることができる前に、難読化を乗り越えるために人による攻撃が必要になる。そのようなアプローチは大量の時間がかかることが避けられず、したがって、連続するモバイル・ガードの間の「信頼できる間隔」が十分に短いとすると、そのアプローチは効果的でなくなる。換言すれば、モバイル・ガードが頻繁に置き換えられるので、このアプローチが意味を持つほど十分な時間がない。したがって、難読化プロセスは、モバイル・ガードを当該モバイル・ガードが別のモバイル・ガードによって置き換えられる前の時間間隔に不正に変更されることか

ら保護する。

【００５４】

復号化された映画データが記憶されるコンピュータ内のメモリ・ロケーションをスパイするオブザーバのリスクが存在する。知られているメモリ・ロケーションが使用される場合、データがコピーされる恐れがある。したがって、特定のメモリ・ロケーションを特定すること（ロケーション・ベースの特定）によってコードを位置指定することが実行可能であることは望ましくなく、好ましくは、いったんロケーションが使用されたら、それらのロケーションは再使用されるべきでない。また、ＭＰＥＧヘッダのような系列を探すことによってコードが探索される可能性があるパターン・ベースの特定も好ましくは防止されるべきである。

【００５５】

したがって、ビューアはモバイル・ガードによって、スパイすることによってそのビューアの状態が判定されることから保護されることが好ましい。この保護を行うために、モバイル・ガードは、そのような攻撃から保護するための１つ又は複数の保護アルゴリズムをさらに含むことが好ましい。これは、以降、「ランタイム・ビューア難読化」と呼ばれるクライアント上の（例えば、ビューア・プログラム上の）難読化タスクを実行することができ、つまり、ビューアが実行するときにビューア上で難読化が実行される。この難読化タスクは、実行中のビューアのメモリ・イメージを変更する。

【００５６】

このランタイム・ビューア難読化はさらなる発明概念と考えられ、したがって、別の態様から、本発明は、実行中のビューアのメモリ・イメージをランダム化することを含む、実行中のビューアを難読化する方法を提供する。

【００５７】

ランタイム難読化は以下の技術のうちの１つ又は複数を含むことができる。

【００５８】

コード再配置は、コード・ブロックをメモリ中であちこちに移動させることを含む。プログラムが実行されるとき、モバイル・ガードは、コードをメモリのその他の部分に移動させ、その場合、そのコードは後で実行されることになる。このアルゴリズムは、チェックサムの計算と緊密にインターリーブされることが好ましい。

【００５９】

好ましくは、コード再配置は、（１）プログラム内の全ての基本的なビルディング・ブロックを特定し、それを小さな再配置可能なセグメントに分割することと、（２）モバイル・ガードの実行中にこれらのセグメントがメモリ内でランダムなロケーションに再配置されることができ、（３）新しいコード・ロケーションに対応するように全てのジャンプ命令を修正することとによって実行される。結果として、攻撃者は、モバイル・ガードの実行中、変化するメモリ・イメージに直面することになる。セグメントのロケーションはセキュリティ・サーバによって提供されるモバイル・ガードによって決定されるので、セグメントのロケーションは、その場合、特定のメモリ・ロケーションが特定のデータを含むという仮定を利用することができない攻撃者には予測不可能である。

【００６０】

データ再配置は、データを移動することと、そのデータにアクセスする命令を変更することとを含む。この場合もやはり、新しいロケーションはランダムに決定されることができる。

【００６１】

データ隠蔽は、ロケーション及びパターン・ベースの特定の問題に対処する。１つのアプローチは、データの見た目を変えるための（効果的にそのデータをマスクするための）双方向の関数を適用することである。好ましくは、単純なワンタイム・パッド・アプローチが使用される。そのアプローチは、ランダム・データの配列にインデックスを作成する新しく生成されたモジュロ関数を含むことができる。ランダム・データは、ランダムな部分とセンシティブな部分の間にＸＯＲ演算子を適用することによってセンシティブなデー

タを変更するために使用されることができる。好ましくは、それは、これらと、センシティブなデータのアドレスの部分との間に適用される。

【００６２】

１つのアプローチは、センシティブなデータがスクランブルされた形態で記憶され、必要とされるときにアンスクランブルされ、次いで再スクランブル又は削除されるようにデータをスクランブル（マスク）及びアンスクランブルすることである。しかし、これは、データがアンスクランブルされるときに短い好機を確かに残す。

【００６３】

しかし、データがプロセッサのレジストリ内に入るまでアンスクランブルを遅らせるためのストリーム処理を利用することが可能である。

【００６４】

したがって、実際のコンテンツ・デコーダは、それが新しいデータを必要とするときに最後の復号化操作を実行するように修正されることができる。これは、いかなる復号化されたデータもメイン・メモリ内にいっさい存在しないことを意味する。それは以下のステップを使用して提供されることができる。

【００６５】

ａ）必要に応じて最後の復号化・ステップを実行するようにモバイル・ガードがデコーダを修正する。

【００６６】

ｂ）次の暗号化されたセグメントが取得される。

【００６７】

ｃ）暗号化されたセグメントに対するメディア・キーが取得される。

【００６８】

ｄ）どのようにデコーダが修正されたかに応じて復号化・ストリームが生成され、メモリ内のランダムな場所に配置される。

【００６９】

ｅ）次にデコーダが必要に応じて一度に１バイト又は１ワードを読み、それらを復号化する。

【００７０】

コード多様化は、実行中にクライアント・プログラム上でモバイル・ガードによって実行される操作を含む。実行される操作は、そのコードの意味を変えることなしにそのコードが異なる命令から構成されるようにコードを変更する。これは、パターン・ベースの特定を防止するためである。以下のステップのうちの１つ又は複数が実行されることができる。

【００７１】

コンテキスト独立命令が挿入されることができる。これらは、その命令の入力コンテキストがプログラム内のコンテキストと共有されることができるが、その命令の出力コンテキストはプログラム内のいかなる入力コンテキストとも異なる命令である。それらの命令はプログラムのいかなる入力コンテキストも変更できないので、それらの命令が何を処理するかは問題にならない。

【００７２】

コンテキスト依存命令は、同じ機能を実行する命令によって置き換えられることができる。これは遂行することがより難しいが、それらがデータフロー分析によって特定されることができないのでそれはより効果的でもあることが理解されるであろう。

【００７３】

行われることができる機能的な独立した変更は、命令の実行の順序を変更することと、一時変数を有するか又は有さない命令を挿入することと、メモリ内で命令を並べ替えることと、制御フローの変更を行うこととを含む。

【００７４】

機能的な非独立な変更は、機能及び副作用を元のままに保つために注意を要する。それ

らの変更は、命令を機能的な等価物で置き換えることと、恒等関数を導入することと、リテラル値を任意に初期化し、元のリテラルと一致するようにその値を修正する操作を実行する命令によってリテラル値が置き換えられように演算子を導入することとを含む。また、目的の場所へのコピーを新しく作成された変数のコピーによって置き換えるように変数が導入されることができる。

【００７５】

ハードウェア・ベースのビューアの解決法が使用される一実施形態、例えば、ＴＶセット・トップ・ボックスにおいて、ビューアの配布者は、ビューア・ソフトウェアだけでなく、ビューア環境、すなわちハードウェア及びオペレーティング・システムも制御する。したがって、概して、ハードウェア・ベースのビューアは、純粋にソフトウェア・ベースの解決法よりもより一層完全なやり方でモバイル・ガードによってチェックされることができる。この実施形態において、モバイル・ガードにおけるチェックサム・アルゴリズムはビューア・ソフトウェアをチェックすることに限定されず、オペレーティング・システム及びハードウェアの様々な側面もチェックすることができる。

【００７６】

したがって、システムはハードウェア・ベースのビューアに関連して２通りに使用されることができる。第１に、システムは、高価な不正防止ハードウェアに基づく解決策を置き換えるために使用されることができ。第２に、システムは、不正防止ハードウェアが危険にさらされているに違いない場合に機能を開始する追加的なセキュリティ対策を提供することができる。

【００７７】

本発明は個々に暗号化されるドキュメントのセグメントと「モバイル・ガード」の概念の使用との組合せに関することが好ましいことが認識されるであろう。したがって、さらに別の態様から見て、本発明は、

（ａ）著作物のそれぞれの時間的に区切られたセグメントに対応する一連の異なるキーを使用して著作物を暗号化するステップと、

（ｂ）クライアントの状態の関数である結果を有するアルゴリズムを含むソフトウェア・コードをセキュリティ・サーバからクライアントに送信するステップと、

（ｃ）クライアントにおいて当該コードを実行し、結果をセキュリティ・サーバに返すステップと、

（ｄ）結果が未修正のビューアを示すかどうかを判定するステップと、

（ｅ）セグメントをサーバからビューアに送信するステップと、

（ｆ）結果が未修正のビューアを示す場合に、送信されたセグメントに対応するキーを安全なリモート・サーバからビューアに安全にストリーミングするステップと、

（ｇ）キーを使用してセグメントを復号化するステップと

を含む、メディア著作物をクライアントに送信する方法を提供する。

【００７８】

ステップが上で与えられる順序でそれらのステップが実行されることができるが、ステップの少なくとも一部は異なる順序で、又は同時に実行されることができることが理解されるであろう。例えば、セグメントがキーの前に、キーと共に、又はキーの後で伝達されるようにステップ（ｅ）は、ステップ（ｂ）、（ｃ）、（ｄ）又は（ｆ）と同時に実行されることができる。しかし、キーは、セグメントが復号化される前に利用可能でなければならない。

【００７９】

一実施形態において、方法は、ステップ（ｂ）から（ｇ）までが繰り返されるさらなるステップ（ｈ）を含む。

【００８０】

しかし、概して、送信されるソフトウェア・コードは、例えば３０秒未満の特定の「存続期間」又は「信頼できる間隔」を有する。その一方、概して、セグメントはソフトウェア・コードの存続期間よりも頻繁に、例えば毎秒１回送信される。したがって、新しいソ

フトウェア・コードはセグメントが送信される度に送信される必要はないが、概して、現在のソフトウェア・コードの存続期間が満了し次第送信されることのみ必要とする。したがって、概して、ステップ（ｅ）から（ｇ）までは、ステップ（ｂ）が繰り返されるときに新しいソフトウェア・コードが要求されるまで繰り返される。このように、１つのソフトウェア・コード（モバイル・ガード）が多くのキーの配信を保護する。

【００８１】

コードの実行と、結果が未修正のビューアを示すかどうかの判定と（ステップｃ及びｄ）は各ソフトウェア・コードに対して２回以上行われることができるが、概して、ソフトウェア・コードの存続期間中にそれを１回行うことだけが必要である。したがって、概して、ステップ（ｃ）及び（ｄ）は、ステップ（ｂ）が繰り返された後にのみ繰り返される。

【００８２】

さらに別の態様から見て、本発明は、

（ａ）著作物のそれぞれの時間的に区切られたセグメントに対応する一連の異なるキーを使用して著作物を暗号化するステップと、

（ｂ）クライアントの状態の関数である結果を有するアルゴリズムを含むソフトウェア・コードをセキュリティ・サーバからクライアントに送信するステップと、

（ｃ）クライアントにおいて当該コードを実行し、結果をセキュリティ・サーバに返すステップと、

（ｄ）結果が未修正のビューアを示すかどうかを判定するステップと

を含み、

（ｅ）セグメントをサーバからビューアに送信するステップと、

（ｆ）送信されたセグメントに対応するキーを安全なリモート・サーバからビューアに安全にストリーミングするステップと、

（ｇ）取得されたメディア・キーを使用してセグメントを復号化するステップと、

（ｈ）ステップ（ｄ）が修正されたビューアを示す場合にさらなるキーが送信されることを防止し、ステップ（ｄ）が修正されたビューアを示さない場合にステップ（ｅ）から（ｇ）までを繰り返すステップと

をさらに含む、メディア著作物をクライアントに送信する方法を提供する。

【００８３】

好ましくは、方法は、ステップ（ｂ）から（ｄ）までを繰り返すステップ（ｉ）をさらに含む。

【００８４】

ステップが上で与えられる順序でそれらのステップが実行されることができるが、ステップの少なくとも一部は異なる順序で、又は同時に実行されることができることが理解されるであろう。実際、一部のステップは、その他のステップよりも多い回数実行されることができる。

【００８５】

ステップ（ｂ）から（ｄ）までは、ステップ（ｅ）から（ｈ）までとは独立して実行されることができ、それらのステップと同時に実行されることが好ましい。上述のように、概して、ソフトウェア・コードは多くのセグメント及びキーの送信を包含する存続期間を有する。したがって、概して、（ステップ（ｉ）で述べられた）ステップ（ｂ）から（ｄ）までの繰り返しは、（ステップ（ｈ）で述べられた）ステップ（ｅ）から（ｇ）までの繰り返しよりも少ない頻度で実行される。好ましくは、ステップ（ｉ）は、ソフトウェア・コードの存続期間が満了した場合にのみ実行される。

【００８６】

本発明は、そのようなストリーミングされたメディアを受信するように構成されたクライアントと、さらにサーバ構成とを両方組み合わせて及び別々に含む、上述のように動作するように構成された装置にも及ぶ。したがって、さらに別の態様から見て、本発明は、

（ａ）著作物をクライアントに送信するための手段と、

（ｂ）クライアントの状態の関数である結果を有するアルゴリズムを含むソフトウェア・コードをセキュリティ・サーバからクライアントに送信するための手段と、
（ｃ）結果を受信し、結果が未修正のクライアントを示すかどうかを判定するための、セキュリティ・サーバに関連する手段と
を含む、メディア著作物をクライアントに配信するためのシステムを提供することができる。

【００８７】

別の態様は、映画などの著作物を再生するためのクライアント、例えばビューアを提供し、当該クライアントは、リモートのソースから著作物を受信し、アルゴリズムを含むソフトウェア・コードを受信し、クライアント上でアルゴリズムを実行し、リモートのソースにアルゴリズムの結果を返し、それによってリモートのソースにクライアントのインテグリティを示し、ドキュメントの再生を可能にするように構成される。

【００８８】

好ましくは、クライアントは、リモートのソースによってそのクライアントに供給されたキーを使用して著作物を復号化すること、又は著作物のセグメントを復号化することによって著作物の再生を可能にすることが好ましい。好ましくは、クライアントは一連のキーを要求するように構成され、順番にキーを使用して著作物の連続したセクションを復号化し、それらの連続したセクションはそのとき連続的な表示として再生される。好ましくは、上述のように、キーの供給はクライアントがそのクライアントのインテグリティをソースに示すことによって決まる。

【００８９】

本発明は、それによってドキュメントがクライアントに配信され、ビューアがそのビューアのインテグリティをソースに示す場合にのみ再生されることができる、クライアントと組み合わせて上述のように著作物を配信するためのシステムの組合せにも及ぶ。

【００９０】

従来技術のソフトウェアによる解決法とは対称的に、本発明は、プログラム・コードの中か、それともメディア・ドキュメントの中かに関わらず、ユーザに対して利用可能にされるデータ内に含まれる秘密に依存しないことが認識されるであろう。本発明は、コピーの試みの早期検出を可能にし、コンテンツ・プロバイダがメディア・ドキュメントの価値ある部分がコピーされることができる前に対策を開始することを可能にする。

【００９１】

モバイル・ガードを使用してシステムのインテグリティをチェックする概念は（定義されたような）ドキュメントのクライアントへの送信に留まらないその他の用途を有することも認識された。概して、その概念は、入力データに対する計算を実行する制御されていない環境内で実行されるコードのインテグリティ及び信憑性を検証するために使用されることができる。その概念は、人がデータが処理されるやり方を変更することをそのことが検出されることなしに防止するために使用されることができる。したがって、メディア・ビューアに関連する上の検討は任意のクライアント・プログラムに適用されることができる。用途は、ゲーム、銀行業務、オーディオなどを含む。

【００９２】

したがって、さらに別の態様から見て、本発明は、クライアント・プログラムの状態によって決まる結果を有するアルゴリズムを含むソフトウェア・コード（モバイル・ガードなど）を安全なソースから、クライアント・プログラムを実行するクライアント・コンピュータに送信することと、ソフトウェア・コードを実行することと、それによってソースがクライアント・プログラムのインテグリティを判定することができる結果をソースに返すこととを含む。本発明は、そのような方法に従って動作するように構成された装置にも及ぶ。

【００９３】

本発明のこの態様は、特にモバイル・ガードに関して、上述の好ましい特徴のいずれか又は全てを使用することができる。メディア著作物に関する上の言及は、サーバとクライ

アントの間で送信される時間的なペイロード・データに同様に当てはまる。したがって、サービス・プロバイダは、同じやり方でユーザのクライアントの協力を強制することができ、協力が停止するか、又は不正な変更が検出されるかのいずれかの場合にさらなるペイロード・データを供給しないことができる。

【００９４】

したがって、サーバと通信している任意のクライアントはそのクライアントのインテグリティを継続的にチェックさせることができることが理解されるであろう。したがって、本発明は、制御されていない環境内で動作するクライアントが信頼されることができるようにする。クライアントのインテグリティが損なわれたことが明らかになる場合、対応が取られることができる。例えば、クライアントとの通信が終了される可能性があり、（上述のメディア・ストリーミング・アプリケーションと同様に）復号化のキーの提供が一時中止される可能性があり、及び／又は（例えば、銀行業務システムに対する疑わしい不正な攻撃の場合に）証拠を収集するためのステップが行われる可能性がある。

【００９５】

本発明は、機密性及び不正行為が通常は問題ではないが、ソフトウェアの正しい実行が問題である分散計算の状況において有用である。したがって、モバイル・ガードは、クライアント（そのクライアントのソフトウェア、及び必要に応じてハードウェアの両方）の意図的な又は意図的でない修正から保護するために使用されることができる。したがって、分散コンピューティングのジョブを起動するインスタンスはモバイル・ガードを使用して、計算を実行するリモート・ノードにおけるクライアントの正しい動作をチェックすることができる。

【００９６】

オンライン・ゲームとの関係で、クライアント・プログラムの修正は、制御されない場合に顧客の不満の原因となり、収益の損失につながる可能性がある不正行為を可能にする可能性がある。関係するデータが機密ではなく、（メディア著作物と同様に）そのデータを記録するポイントがほとんどないので、クライアント・ソフトウェアのインテグリティを検証するだけで通常は十分である。ゲームがクライアント・サーバ・ベースで動作される場合、モバイル・ガードが上述のように適用されることができる。ユーザがモバイル・ガードとの協力を許さない場合、ユーザは、全体的なゲームの状態に関するアップデートを拒否される可能性がある。

【００９７】

ホーム・バンキングの場合、第三者が機密データにアクセスしないことを保証するためにモバイル・ガードが使用されることができる。通常は普通のユーザはそのユーザのクライアント・プログラムを修正することに関心がないが、ユーザは中間者攻撃の被害者になる可能性がある。したがって、銀行業務サーバは、ホーム・バンキング・クライアントのインテグリティ及び信憑性を検証するためにモバイル・ガードを使用する可能性があり、それは銀行業務サーバの公開キーも含むことができる。この公開キーは、ホーム・バンキング・クライアントから銀行業務サーバに渡される全てのデータを暗号化するために使用され、モバイル・ガードのインテグリティが保証されるので、ユーザはそのユーザのデータが機密に保たれることを確信することができる。

【００９８】

本発明は、上述の方法を使用するように構成された装置と、コンピュータをそのようなやり方で動作させるための命令を含むソフトウェア製品とにまで及ぶ。本発明は、上述の本発明の態様に従ってデータがクライアントに供給されるサーバ・クライアントの組合せ及び／又はネットワークにも及ぶ。

【発明を実施するための最良の形態】

【００９９】

ここで、本発明のいくつかの実施形態が、添付の図面を参照して単に例として説明される。

【０１００】

図２から認識されるであろうように、クライアントは、ストリーミング・サーバ１１又は代替的にローカルの記憶メディア、例えばＣＤ１２からストリーミングされるメディア（例えば、映画）を見るために使用されることができるビューア１０を提供される。システムのこれらのコンポーネントのそれぞれは信頼できる環境１３の外にある。信頼できる環境内にあるのは、暗号化されていない映画１４と、保護された映画１６を生成するための保護ツール１５と、セキュリティ・サーバ１７である。

【０１０１】

図１において示された従来技術のシステムにおけるように、符号化されたメディア・ドキュメントがクライアントに配信される前にコンテンツの所有者は符号化されたメディア・ドキュメントを保護する。しかし、単一のメディア・キーを使用する代わりに、保護ツール１５は、非常に多数（数千）のメディア・キー２０を用いて映画を暗号化する。このプロセスは、暗号化された符号化メディア、すなわち保護された映画１６を生成する。

【０１０２】

メディア・キー２０はそれらのメディア・キーが時間的に拡散されるように配布され、メディア・リソースの表示中にそれらのメディア・キーは、以下で説明されるように要求に応じて間隔をおいて一度に１つずつクライアントに安全にストリーミングされる。このメディア自体は別にストリーミングされる。各キーは数バイト（約１６）だけを含むので、キーをストリーミングするために必要とされるリソースは非常に少ないオーバーヘッドを生じる。

【０１０３】

各キーはムービーのうちの約１秒、又は最大でも数秒だけを復号化するために使用されることができるので、単一のキーのみを取得することはほとんど価値がない。

【０１０４】

本発明の第１の実施形態において、保護された映画は、経路Ａ、ストリーミング・サーバ１１、及びメディア・ストリーム１８を介したデータ・ストリームの形態でクライアントに配信される。さらなる実施形態において、有形のメディア、例えばＣＤ又はＤＶＤ１２が使用される。

【０１０５】

ビューア１０はクライアントのホスト上で実行され、メディア・ストリーム１８を介してストリーミング・サーバ１１から（又はその他の実施形態においてはＣＤ／ＤＶＤから）保護された映画１６を受信するように構成される。表示プロセス中、ビューア１０はセキュリティ・サーバ１７と通信して、保護された映画１６を復号化するために必要なメディア・キー２０をダウンロードする。

【０１０６】

さらに、ビューア１０は、約３０秒の規則的な間隔でモバイル・ガード１９と呼ばれるいくつかのコードもダウンロードする。これらはそれぞれ、セキュリティ・サーバ１７において生成されるアルゴリズムの形態の秘密情報をそれらの中に組み込んでいる。ストリーミング・データ１８を利用するためにはこれらのアルゴリズムの実行が必要である。各モバイル・ガード１９がビューアに転送されるとき、そのモバイル・ガードは秘密のアルゴリズムによって決定された計算を実行し、セキュリティ・サーバに結果を返す。モバイル・ガードは、ビューアが不正に変更されていない場合にのみ計算の結果が正しいやり方で構築される。秘密のアルゴリズムの結果は、ビューアのインテグリティをセキュリティ・サーバに対して証明するチェックサムを含む。

【０１０７】

モバイル・ガードは、機能的に及び空間的に秘密のアルゴリズムと関わり合わされたその他の追加的なアルゴリズムも有することができる。このように、クライアントのコンピュータ／ビューアが追加的なアルゴリズムを実行しない場合は秘密のアルゴリズムが実行されないので、クライアントのコンピュータ／ビューアは追加的なアルゴリズムを実行するように強制されることができる。このようにして、ビューアは十分にチェックされることができる。

【０１０８】
モバイル・ガードによってセキュリティ・サーバ１７に返された結果が期待される結果と一致しない場合、セキュリティ・サーバはビューアへのメディア・キー２０の配布を停止する。ビューア１０がモバイル・ガードを拒否する場合、又は正しい結果が特定の時間内に到着しない場合は同じことが起こる。キー交換プロトコルが後でより詳細に説明される。

【０１０９】
秘密のアルゴリズムは、チェックされるデータ（すなわち、ビューアのコード）の変更を検出する高い確率を有するチェックサムの計算に基づく。図３から認識されるであろうように、（モバイル・ガードにおける使用のための）ランダムに生成されるチェックサム・アルゴリズム２１は、２つのステップ、すなわち、ランダム化される入力の修正２２と、修正された入力に対して実行される知られているチェックサムの計算２３とに分割されたチェックサムの計算を使用する。これらのステップは、ランダム化された秘密のチェックサム・アルゴリズムを一緒に作り上げる。

【０１１０】
入力の修正は、チェックサムの計算２３に入力されることになるデータを並べ替えるモディファイアのランダムな生成を指す。セキュリティ・サーバによってモバイル・ガードが生成されるときに、ランダムな順序が決定される。ビューアによってチェックサム・アルゴリズム２１が実行されるときに、ビューアからの入力プログラム・コードが同じサイズのｎ個のブロックに分割される。次に、入力の修正段階２２において、これらは上述のランダムな順序にシャッフルされる。続いて、この結果がチェックサムの計算段階２３に入力される。このチェックサムの計算段階２３は、知られているＭｅｓｓａｇｅ　Ｄｉｇｅｓｔ　Ａｌｇｏｒｉｔｈｍ（ＭＤ５）を使用する。続いて、チェックサムの計算が実行され、その計算の結果がセキュリティ・サーバに返される。

【０１１１】
チェックサム・アルゴリズム自体は公開されているが、そのアルゴリズムの結果はｎ個のブロックがそのアルゴリズムに入力される順序の関数であることが理解されるであろう。この順序はセキュリティ・サーバに知られており、したがって、セキュリティ・サーバはそのセキュリティ・サーバに返された結果が元のままのビューアを示すかどうかを判定することができる。

【０１１２】
モバイル・ガードは、不正な変更に対して、及びそのモバイル・ガードの内部の働きを探り出すことに対して保護される必要がある。モバイル・ガードの保護の第１の態様は、ビューアがチェックされる必要がある度に新しいバージョンをランダムに生成することである。第２に、モバイル・ガードが使用されているときにビューア環境におけるモバイル・ガードの存続期間が短い（３０秒未満）。モバイル・ガードに対する人による（すなわち、自動化された攻撃と対称的に知的な）攻撃が理論上あり得るが、それらの攻撃は非常に多くの時間を要する。各モバイル・ガードに対して数秒の失効時間を有することによって、何らかの攻撃が完了されることができるよりもかなり前に当該モバイル・ガードが不要になるので、したがって人が支援する攻撃は実質的に不可能になる。

【０１１３】
モバイル・ガードは、自動化された攻撃から守るために上述のように難読化される。

【０１１４】
モバイル・ガードは実行中のビューアのメモリ・イメージをランダム化し、これは本明細書において「ランタイム・ビューア難読化」と呼ばれる。ビューアのコード及びデータ領域がスワップされ、スタックがスクランブルされる。これは以下でより完全に検討される。

【０１１５】
ランタイム・ビューア難読化の効果は、ランタイム・ビューア難読化が復号化された符号化ストリームのメモリ・ロケーションをランダム化し、それによって隠蔽するのでビュ

ーアのランタイム・イメージに対して知的な攻撃のみが実行可能であることを確実にすることである。

【０１１６】

メモリ・アクセスのロケーションをランダム化するために、モバイル・ガードは、ビューアのコード及びデータ領域の構造を修正する。コード及びデータ領域は論理的なセグメントに分割される。セグメントの境界がオペコードの中に配置されないという注意が払われる。

【０１１７】

新しくダウンロードされたモバイル・ガードが制御を受け取った後で、及びストリームの復号化を開始する前に、モバイル・ガードはセグメントを新しい位置に再配置する。このプロセスは、

１．ジャンプ及び分岐命令が制御を再配置された位置に移している

２．読み出し及び書き込み命令が再配置された位置のデータにアクセスしている

ことを確実にするために（ダイナミック・リンカによって実行される再配置と同様の）コード・セグメントの修正を含む。

【０１１８】

セグメントを再配置した後で、モバイル・ガードは、そのモバイル・ガードが次のモバイル・ガードによって置き換えられるまでそのモバイル・ガードの動作を実行する。

【０１１９】

モバイル・ガードは、ビューア内の特定の関数のエントリ・ポイントを知る必要がある。セグメントの新しい位置はセキュリティ・サーバによって知られ、モバイル・ガードに提供される。このように、クライアント側で２つのモバイル・ガードの間で情報を転送する必要はない。

【０１２０】

スタックのスクランブルに関して、スタックは前の関数呼び出しに対するリターン・アドレスを含む。これは、制御フローを探り出すため、又はスタック上のリターン・アドレスを変更することによってビューアの制御フローを変更するためのいずれかに使用される可能性がある。そのような攻撃において、プログラムが呼び出し元の関数に戻ろうとしているときに、プログラムはその代わりにあり得る敵意を持ったコードに制御を移そうとしている可能性がある。

【０１２１】

そのような攻撃に対してスタックを保護するために、スタックに新しいリターン・アドレスが追加されるにつれてスタックを徐々にスクランブルする方法が使用される。チェックされるコードは関数呼び出しの後、制御を呼び出し元の関数に戻す前にスタック上の新しいリターン・アドレスをスクランブルするモバイル・ガード内のスクランブル関数に制御を移す。スタックをアンスクランブルするために、何らかのリターン・アドレスを使用する前にモバイル・ガード内の対応するアンスクランブル関数が呼び出される。

【０１２２】

スクランブル関数の実装は、ビューアをチェックするためにモバイル・ガードが必要に応じて生成されるという事実を利用する。これは、各モバイル・ガードにおいて一意的なスクランブル及びアンスクランブル関数が生成されることを可能にする。基本的に、スクランブル関数は、ビューアのスタック上のリターン・アドレスとＸＯＲ演算される、セキュリティ・サーバによって生成され、モバイル・ガードに含まれる１組のランダム・データから構成される。ランダム・データのどの部分を使用するかを選択するために、１組のランダム・データにインデックスを計算するために簡単な数学的な関数が適用される。

【０１２３】

したがって、ビューアはモバイル・ガードによって、（制御フローの位置と変数の内容とを含む）そのビューアの状態が（上述のように）スパイすることによって判定されることから保護される。

【０１２４】

メディア・キーは、約１秒に１回のレートでビューアに送信される。これは、ランダム・データ・ジェネレータと、ビューアに知られているセキュリティ・サーバの公開キーとを使用するキー交換プロトコルを使用して行われる。次のメディア・キーを取得することが必要なとき、ビューア１０は１６バイトのランダム・データを生成し、それらのデータをセキュリティ・サーバ１７の公開キーを用いて暗号化する。次に、暗号化されたデータが、セキュリティ・サーバに送信されるキーの要求に含められる。

【０１２５】

セキュリティ・サーバは要求を検査し、モバイル・ガードがビューア内で全てが正しいことを示す場合にのみその要求を認める。モバイル・ガードが全て問題ないことを示す場合に、セキュリティ・サーバはランダム・データを抽出し、そのランダム・データを要求されたキーとＸＯＲ演算し、結果をビューアに送り返す。

【０１２６】

ビューアが結果を受信するとき、ビューアは、当該結果を最初のキーの要求において提供された同じランダム・データとＸＯＲ演算することによって当該結果から要求されたキーを抽出する。

【０１２７】

このプロトコルは、ビューアのソース・コード内に隠蔽されたいかなる秘密キーもなしに、暗号化された符号化メディア・ストリームを復号化するやり方を提供する。キーの存続期間はほんの数秒であり、そのことは、１つ又はいくつかの秘密キーの抽出があった場合に安全なストリーミング・プロセスが単一障害点をなすことを防止する。

【０１２８】

クライアントによって実行される事実上２つの別個のスレッドが存在することが理解され、これらは図４のフロー・チャートでまとめられる。

【０１２９】

第１のスレッドは検証である。クライアントはモバイル・ガードを受信し、続いてそのモバイル・ガードがクライアント・プログラムを検証する。いったん検証が確認されると、モバイル・ガードが失効するまで、引き続く信頼できる間隔の間にｎ個のキーが受信されることができる。次に、スレッドは新しいモバイル・ガードを用いて繰り返されなければならない。

【０１３０】

このスレッドに平行して実行されているのは表示スレッドである。各キーに対してメディア・ストリームのセグメントが受信され、復号化され、表示される。

【０１３１】

図５は、サーバの動作を要約する。キーの要求を受信すると、サーバは、モバイル・ガードがまだ有効である場合（すなわち、モバイル・ガードがまだそのモバイル・ガードの信頼できる間隔内にある場合）かつその場合に限ってキーをクライアントに送信する。モバイル・ガードが失効した場合、新しいモバイル・ガードがクライアントに送信され、このモバイル・ガードがクライアントを検証するために使用される。結果が正しくない場合、クライアントは不正に変更されたと見なされ、その場合、キーの送信が停止される。結果が満足できる場合、新しい信頼できる間隔が始まり、その信頼できる間隔の間にキーがクライアントに送信される。

【図面の簡単な説明】

【０１３２】

【図１】上述の従来技術のメディア・ストリーミング・システムの概略図である。

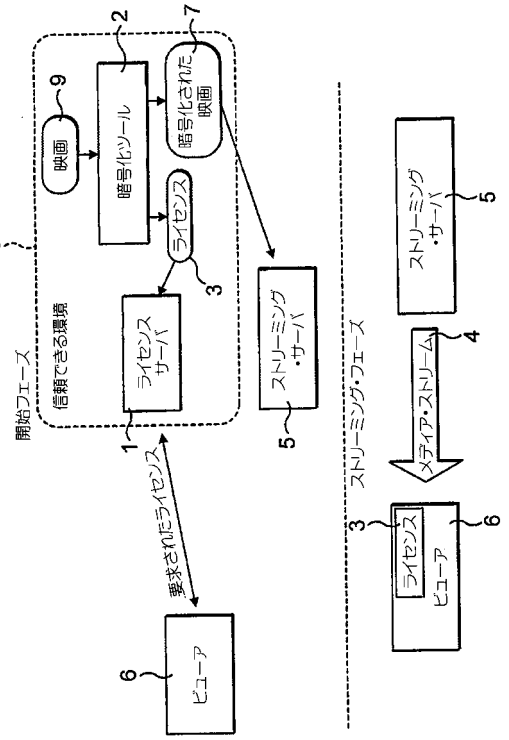
【図２】本発明の第１の実施形態の概略全体図である。

【図３】実施形態において使用されるランダムに生成されるチェックサム・アルゴリズムのコンポーネントを示す概略図である。

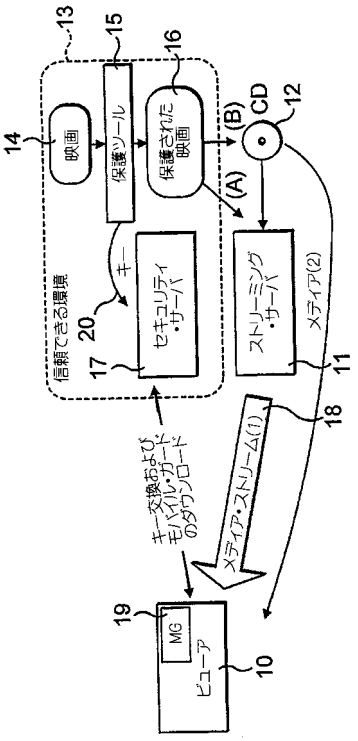
【図４】実施形態の動作を示すフロー・チャートである。

【図５】実施形態において使用されるサーバ・アルゴリズムを示すフロー・チャートである。

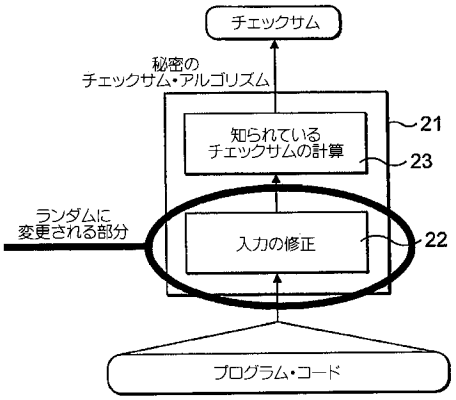
【図１】


開始フェーズ
信頼できる環境
8
映画
9
暗号化ツール
2
暗号化された映画
7
ライセンス
3
ライセンスサーバ
1
ストリーミング・サーバ
5
要求されたライセンス
ビューア
6
ストリーミング・フェーズ
ストリーミング・サーバ
5
メディア・ストリーム
4
ライセンス
3
ビューア
6

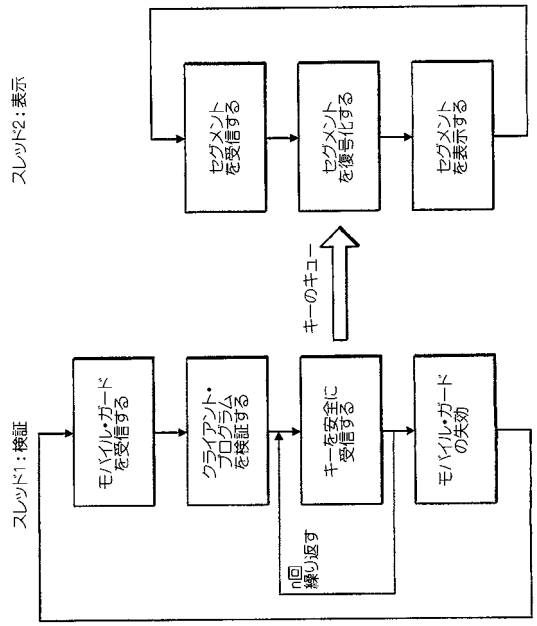
【図２】


信頼できる環境
13
映画
14
保護ツール
15
保護された映画
16
(A)
(B)
CD
12
キー
20
セキュリティ・サーバ
17
ストリーミング・サーバ
メディア(2)
11
キー交換およびモバイル・ガードのダウンロード
メディア・ストリーム(1)
18
MG
ビューア
19
10

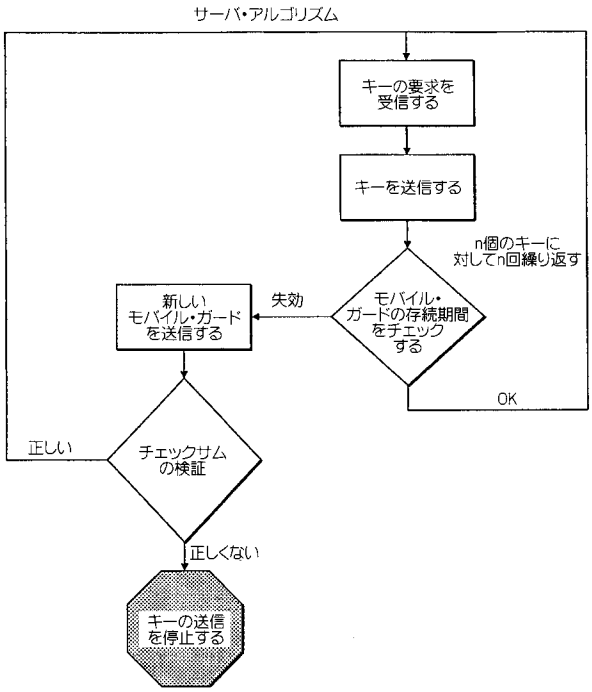
【図３】


チェックサム
秘密のチェックサム・アルゴリズム
知られているチェックサムの計算
21
23
ランダムに変更される部分
入力の修正
22
プログラム・コード

【図４】


スレッド2：表示
セグメントを受信する
セグメントを復号化する
セグメントを表示する
キーのキュー
スレッド1：検証
モバイル・ガードを受信する
クライアント・プログラムを検証する
キーを安全に受信する
モバイル・ガードの失効
n回繰り返す

【図５】



【手続補正書】
【提出日】平成19年8月10日(2007.8.10)
【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】
メディア著作物をクライアントに送信する方法であって、
（ａ）前記著作物のそれぞれの時間的に区切られたセグメントに対応する一連の異なるキーを使用して前記著作物を暗号化するステップと、
（ｂ）第１のキーを安全なサーバから前記クライアントに安全に送信し、対応するセグメントをサーバから前記クライアントに送信するステップと、
（ｃ）前記クライアントにおいて、前記対応するセグメントを復号化するために前記第１のキーを使用するステップと、
（ｄ）前記クライアントにおいて、復号化された部分を表示するステップと、
（ｆ）さらなるセグメント及びキーについてステップ（ｂ）から（ｄ）までを繰り返すステップと
を含み、
前記キーが、ランダム・データ・ジェネレータと、前記クライアントに知られている前記安全なサーバの公開キーとを使用するキー交換プロトコルを使用して送信される、方法。
【請求項２】
前記クライアントが、前記ランダム・データ・ジェネレータによって生成されたランダ

ム・データを前記安全なサーバの前記公開キーを用いて暗号化して暗号化されたデータを生成し、前記安全なサーバからのキーを要求し、前記暗号化されたデータは前記キーの前記要求と共に前記安全なサーバに送信される、請求項１に記載の方法。

【請求項３】

前記安全なサーバが前記ランダム・データを復号化及び抽出し、前記抽出されたランダム・データを使用して前記要求されたキーを暗号化する、請求項２に記載の方法。

【請求項４】

前記安全なサーバが、前記キーを暗号化するために前記ランダム・データを使用する関数を実行する、請求項３に記載の方法。

【請求項５】

前記キーと前記ランダム・データとがＸＯＲ演算される、請求項３又は４に記載の方法。

【請求項６】

前記暗号化された要求されたキーが前記クライアントに送信され、前記クライアントが前に生成された前記ランダム・データを使用して前記要求されたキーを抽出する、請求項３乃至５のいずれかに記載の方法。

【請求項７】

前記クライアントが前記ランダム・データを生成する、請求項２乃至６のいずれかに記載の方法。

【請求項８】

各キーの要求に１６バイトのランダム・データが使用される、請求項２乃至７のいずれかに記載の方法。

【請求項９】

前記キーが、いかなるキーも２つ以上のセグメントを復号化するために使用することができないように暗号として互いに独立して配布される、前記請求項のいずれかに記載の方法。

【請求項１０】

前記クライアントが前記ドキュメントを受信する権利を与えられていることのチェックの後でのみキーが供給される、前記請求項のいずれかに記載の方法。

【請求項１１】

前記キーが、前記安全なサーバと前記クライアントの間の協力を強制するために使用される、前記請求項のいずれかに記載の方法。

【請求項１２】

各キーが所定の長さのセグメントに対応する、前記請求項のいずれかに記載の方法。

【請求項１３】

前記安全なサーバが前記クライアントから離れている、前記請求項のいずれかに記載の方法。

【請求項１４】

各キーが前記クライアントによって個々に要求されなければならない、前記請求項のいずれかに記載の方法。

【請求項１５】

前記クライアントが不正に変更されていないことを保証するために前記クライアントのインテグリティをチェックするステップをさらに含む、前記請求項のいずれかに記載の方法。

【請求項１６】

前記安全なサーバが、クライアントの修正が検出される場合、及び／又は前記クライアントのインテグリティ・チェックが成功でない場合にキーの供給を停止するように構成される、請求項１５に記載の方法。

【請求項１７】

前記クライアントの前記インテグリティが（明細書において定義される）モバイル・ガ

ードによってチェックされる、請求項１５又は１６に記載の方法。
【請求項１８】
各キーが、前記クライアントの前記インテグリティを成功裏に検証したモバイル・ガードの信頼できる間隔の間にのみ送信される、請求項１７に記載の方法。
【請求項１９】
前記クライアントが修正されていない場合にのみ正しい結果を返すランダムに生成されるアルゴリズムの使用を含む、請求項１５乃至１８のいずれかに記載の方法。
【請求項２０】
たとえキーの前記供給が停止されたとしても送信が継続することができるように前記セグメントが前記対応するキーとは独立に送信される、前記請求項のいずれかに記載の方法。
【請求項２１】
前記メディア著作物が記録物である、前記請求項のいずれかに記載の方法。
【請求項２２】
前記メディア著作物がライブ・パフォーマンスである請求項１乃至２１のいずれかに記載の方法。
【請求項２３】
前記メディア著作物がリモート・サーバから前記クライアントにストリーミングされる、前記請求項のいずれかに記載の方法。
【請求項２４】
データをクライアントに送信する方法であって、
（ａ）前記データを前記クライアントに送信するステップと、
（ｂ）前記クライアントの状態の関数である結果を有するアルゴリズムを含むソフトウェア・コードをセキュリティ・サーバから前記クライアントに送信するステップと、
（ｃ）前記クライアントにおいて前記コードを実行し、結果を前記セキュリティ・サーバに返すステップと、
（ｄ）前記結果が未修正のクライアントを示すかどうかを判定するステップと
を含む、方法。
【請求項２５】
前記データがメディア著作物である、請求項２４に記載の方法。
【請求項２６】
ステップ（ｄ）が実行されるまで前記クライアントが前記データを使用することが防止される、請求項２４又は２５に記載の方法。
【請求項２７】
前記結果が未修正のビューアを示さない場合に前記データの及び／又は前記データを復号化するために必要なキーの送信を停止するステップ（ｅ）をさらに含む、請求項２４、２５又は２６に記載の方法。
【請求項２８】
前記コードが、前記クライアントのプログラム・コード及び／又はメモリ・イメージが入力されるチェックサムの計算を含む、請求項２４乃至２７のいずれかに記載の方法。
【請求項２９】
前記チェックサムの計算は前記チェックサムの計算の入力に乱数を含む、請求項２８に記載の方法。
【請求項３０】
前記クライアントは前記乱数を前記セキュリティ・サーバの公開キーを用いて暗号化し、前記暗号化された乱数はメディア・キーの要求及び計算されたチェックサムと共に前記セキュリティ・サーバに送信され、前記セキュリティ・サーバは前記乱数を復号化し、前記復号化された乱数を使用して前記メディア・キーを暗号化し、前記セキュリティ・サーバは前記乱数を使用して前記セキュリティ・サーバ自身の前記チェックサムの計算を更新し、続いて前記セキュリティ・サーバは前記チェックサムの２つの値を比較する、請求項

２９に記載の方法。
【請求項３１】
前記２つの値が等しい場合かつその場合に限り、前記暗号化されたメディア・キーが前記クライアントに送信され、その結果、前記クライアントは前記メディア・キーを復号化することができる、請求項３０に記載の方法。
【請求項３２】
前記２つの値が等しくない場合に、前記クライアント・ビューアが不正に変更されたと判定される、請求項３１に記載の方法。
【請求項３３】
前記コードが前記ビューア上で（１つ又は複数の）難読化タスクを実行する、請求項２４乃至３２のいずれかに記載の方法。
【請求項３４】
前記（１つ又は複数の）難読化タスクが、実行中のビューアのメモリ・イメージをランダム化することを含む、請求項３３に記載の方法。
【請求項３５】
前記難読化タスクが以下のこと、すなわち、全て明細書において定義される、コード再配置、コード多様化、コード再配置、及びデータ隠蔽のうちの１つ又は複数を含む、請求項３３に記載の方法。
【請求項３６】
前記モバイル・ガードが難読化される、請求項２４乃至３５のいずれかに記載の方法。
【請求項３７】
実行中のビューアを難読化する方法であって、前記実行中のビューアのメモリ・イメージをランダム化することを含む、方法。
【請求項３８】
メディア著作物をクライアントに送信する方法であって、
（ａ）前記著作物のそれぞれの時間的に区切られたセグメントに対応する一連の異なるキーを使用して前記著作物を暗号化するステップと、
（ｂ）前記クライアントの状態の関数である結果を有するアルゴリズムを含むソフトウェア・コードをセキュリティ・サーバから前記クライアントに送信するステップと、
（ｃ）前記クライアントにおいて前記コードを実行し、結果を前記セキュリティ・サーバに返すステップと、
（ｄ）前記結果が未修正のクライアントを示すかどうかを判定するステップと、
（ｅ）セグメントをサーバから前記クライアントに送信するステップと、
（ｆ）前記結果が未修正のクライアントを示す場合に、前記送信されたセグメントに対応するキーを安全なリモート・サーバから前記クライアントに安全にストリーミングするステップと、
（ｇ）前記キーを使用して前記セグメントを復号化するステップと
を含む、方法。
【請求項３９】
それぞれのアルゴリズムを含むソフトウェア・コードが関連する信頼できる間隔を有し、前記信頼できる間隔の間に複数のキーが前記クライアントにストリーミングされる、請求項３８に記載の方法。
【請求項４０】
ステップ（ｂ）から（ｇ）までが繰り返されるさらなるステップ（ｈ）をさらに含む、請求項３８又は３９に記載の方法。
【請求項４１】
メディア著作物をクライアントに送信する方法であって、
（ａ）ドキュメントのそれぞれの時間的に区切られたセグメントに対応する一連の異なるキーを使用して前記著作物を暗号化するステップと、
（ｂ）前記クライアントの状態の関数である結果を有するアルゴリズムを含むソフトウ

ェア・コードをセキュリティ・サーバから前記クライアントに送信するステップと、
（ｃ）前記クライアントにおいて前記コードを実行し、結果を前記セキュリティ・サーバに返すステップと、
（ｄ）前記結果が未修正のクライアントを示すかどうかを判定するステップと
を含み、
（ｅ）セグメントをサーバから前記クライアントに送信するステップと、
（ｆ）前記送信されたセグメントに対応するキーを安全なリモート・サーバから前記クライアントに安全にストリーミングするステップと、
（ｇ）前記取得されたメディア・キーを使用して前記セグメントを復号化するステップと、
（ｈ）ステップ（ｄ）が修正されたクライアントを示す場合にさらなるキーが送信されることを防止し、ステップ（ｄ）が修正されたクライアントを示さない場合にステップ（ｅ）から（ｇ）までを繰り返すステップと
をさらに含む、方法。
【請求項４２】
ステップ（ｂ）から（ｄ）までを繰り返すステップ（ｉ）をさらに含む、請求項４１に記載の方法。
【請求項４３】
クライアント・プログラムの状態に依存するアルゴリズムを含むソフトウェア・コードを安全なソースから、前記クライアント・プログラムを実行するクライアント・コンピュータに送信するステップと、前記ソフトウェア・コードを実行するステップと、それによって前記ソースが前記クライアント・プログラムのインテグリティを判定することができる結果を前記ソースに返すステップとを含む、クライアント・プログラムのインテグリティをチェックする方法。
【請求項４４】
前記クライアント・プログラムが以下のこと、すなわち、インターネット・バンキング、オンライン・ゲーム、及び分散計算のうちの１つにおいて使用される、請求項４３に記載の方法。
【請求項４５】
前記請求項のいずれかに記載の方法に従って動作するように構成された装置。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2006/002619

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N7/16 H04N5/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	-/--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 March 2007	30/03/2007

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fantini, Federico

4

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2006/002619

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	INTERNET STREAMING MEDIA ALLIANCE: "Internet Streaming Media Alliance Encryption and Authentication Specification Version 1.0" INTERNET CITATION, [Online] February 2004 (2004-02), XP002376448 Retrieved from the Internet: URL:http://www.isma.tv> [retrieved on 2006-04-10]	1-8, 14-17,39
Y	page 9, line 1 - page 10, line 2 page 10, line 37 - line 39 page 14, line 14 - line 18 page 18, line 30 - line 37 page 21, paragraph 8.1 page 22, line 20 - line 29 page 23, line 12 - line 13 page 34, line 4 - page 35, line 11 page 35, line 24 - line 27 page 37, paragraph A.3 - page 38 page 9; figures 5.2-1 page 13; figures 6.0-1	9-13,21, 32-36
A	page 34; figures a-1	18-20, 22-31, 37,38

Y	US 2002/164023 A1 (KOELLE KATHARINA VERONIKA [US] ET AL) 7 November 2002 (2002-11-07)	9-13,21, 22,27-36
X	abstract paragraph [0004] - paragraph [0005] paragraph [0010] - paragraph [0011] paragraph [0039] - paragraph [0040] paragraph [0046] - paragraph [0048] paragraph [0056] paragraph [0062] paragraph [0064] - paragraph [0065]	18-20, 37,38
A	figures 1,9	1-8, 14-17, 23-26,39

Y	CHANG H ET AL: "Protecting Software Code by Guards" LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER VERLAG, BERLIN, DE, vol. 2320, 10 June 2002 (2002-06-10), pages 160-175, XP002245264 ISSN: 0302-9743 the whole document	22,27-31

	-/--	

4

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2006/002619

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MACQ B M ET AL: "CRYPTOLOGY FOR DIGITAL TV BROADCASTING" PROCEEDINGS OF THE IEEE, IEEE. NEW YORK, US, vol. 83, no. 6, 1 June 1995 (1995-06-01), pages 944-957, XP000518745 ISSN: 0018-9219 the whole document	1-17, 32-36,39
A	MESSERGES T S ET AL ASSOCIATION FOR COMPUTING MACHINERY: "DIGITAL RIGHTS MANAGEMENT IN A 3G MOBILE PHONE AND BEYOND" PROCEEDINGS OF THE 3RD. ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT. DRM 2003. WASHINGTON, DC, OCT. 27, 2003, PROCEEDINGS OF THE ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT. (DRM), NEW YORK, NY : ACM, US, 27 October 2003 (2003-10-27), pages 27-38, XP001238173 ISBN: 1-58113-786-9 the whole document	1-17, 32-36,39
A	US 2005/120125 A1 (MORTEN GLENN A [US] ET AL) 2 June 2005 (2005-06-02) paragraph [0014] paragraph [0042] - paragraph [0043] paragraph [0052] paragraph [0091]	1-17, 32-36,39
A	EP 1 246 463 A (MATSUSHITA ELECTRIC IND CO LTD [JP]) 2 October 2002 (2002-10-02) abstract paragraph [0003] paragraph [0010] - paragraph [0014] paragraph [0017] - paragraph [0019] paragraph [0059] - paragraph [0060] paragraph [0066] - paragraph [0068] paragraph [0070] paragraph [0075] paragraph [0077] - paragraph [0078] figure 7	18-31, 37,38
A	WO 02/21761 A (WIDEVINE TECHNOLOGIES INC [US]) 14 March 2002 (2002-03-14) page 4, line 5 - line 14 page 8, line 11 - line 14 page 8, line 28 - page 9, line 9 page 10, line 8 - line 9 page 12, line 26 - page 13, line 7 page 14, line 6 - line 11 figure 2	18-31, 37,38

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/GB2006/002619

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

International Application No. PCT/GB2006/002619

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-17,32-36,39

Encryption of a media work with multiple encryption keys each associated to a different media work segment.

---

2. claims: 18-31,37,38

Integrity check of a client viewer by a security server using downloadable software code.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2006/002619

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002164023 A1	07-11-2002	NONE	
US 2005120125 A1	02-06-2005	NONE	
EP 1246463 A	02-10-2002	CN 1379377 A	13-11-2002
		CN 1747040 A	15-03-2006
		JP 2002297452 A	11-10-2002
		KR 20020077053 A	11-10-2002
		US 2002141579 A1	03-10-2002
WO 0221761 A	14-03-2002	AU 8875501 A	22-03-2002
		EP 1317839 A2	11-06-2003
		JP 2004511931 T	15-04-2004
		US 7165175 B1	16-01-2007

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 クリスチアン メンク
ノルウェー王国、７０１０ トロンハイム、 タラルツゴールツヴァイテ １０
Ｆターム(参考) 5J104 AA34 DA04 PA07 PA10

【要約の続き】
などのメディア著作物をクライアントに送信する方法を提供する。