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

特許第3748352号

(P3748352)

(45)発行日　平成18年2月22日(2006.2.22)　(24)登録日　平成17年12月9日(2005.12.9)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	550A
G06F 21/00	(2006.01)	G06F	15/00	330Z
H04N 1/387	(2006.01)	H04N	1/387	
H04N 7/167	(2006.01)	H04N	7/167	Z
H04N 7/08	(2006.01)	H04N	7/08	Z

請求項の数 15　(全 17 頁)　最終頁に続く

(21)出願番号　特願平11-357131
(22)出願日　平成11年12月16日(1999.12.16)
(65)公開番号　特開2001-177816(P2001-177816A)
(43)公開日　平成13年6月29日(2001.6.29)
審査請求日　平成14年12月24日(2002.12.24)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100094145
弁理士　小野　由己男
(74)代理人　100094167
弁理士　宮川　良夫
(74)代理人　100106367
弁理士　稲積　朋子
(72)発明者　平野　秀幸
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】データ運用方法、画像生成方法のプログラムを記録する記録媒体、画像復元方法のプログラムを記録する記録媒体

(57)【特許請求の範囲】

【請求項１】

コンテンツ管理者コンピュータがデジタルコンテンツに付加情報を可視的に配置してコンテンツ利用者コンピュータに配布するデータ運用方法であって、

前記コンテンツ管理者コンピュータは、

前記付加情報が可視的に配置される位置を含む前記デジタルコンテンツの一部を部分データ部として複製し、この部分データ部を暗号化して暗号化部分データ部を作成する段階と、

前記デジタルコンテンツに前記付加情報を可視的に配置して付加情報付きデータ部を作成する段階と、

前記部分データ部の前記デジタルコンテンツにおける位置およびサイズに関する画像合成情報と、前記暗号化部分データ部作成時に暗号化に使用した暗号鍵の情報を含む許諾情報とを、前記付加情報付きデータ部に不可視情報として埋め込んで許諾情報付きデータ部を作成する段階と、

前記暗号化部分データ部と前記許諾情報付きデータ部とを合成した合成データを作成しこれを配布する段階と、

を実行するデータ運用方法。

【請求項２】

前記付加情報は、可視的電子透かしとして前記デジタルコンテンツに埋め込まれる、請求項１に記載のデータ運用方法。

【請求項３】
前記デジタルコンテンツに可視的電子透かしとして埋め込まれる付加情報と同等の付加情報を、前記部分データ部に不可視電子透かしとして埋め込み、これを暗号化して暗号化部分データ部を作成する、請求項２に記載のデータ運用方法。
【請求項４】
前記画像合成情報および許諾情報は、秘匿鍵によって暗号化されて前記デジタルコンテンツに不可視情報として埋め込まれる、請求項１～３のいずれかに記載のデータ運用方法。
【請求項５】
前記画像合成情報および許諾情報は、秘匿鍵によって暗号化されて、前記デジタルコンテンツの前記付加情報が可視的に配置される位置を含む部分に不可視電子透かしとして埋め込まれる、請求項４に記載のデータ運用方法。
【請求項６】
前記秘匿鍵は、ユーザ識別情報、ユーザ使用のコンピュータに搭載された機器の識別情報、ユーザ使用のコンピュータに搭載されたＣＰＵ識別情報、前記デジタルコンテンツを格納する記録媒体に固有の識別情報またはユーザ使用のコンピュータに登録されたユーザログイン情報のうちから選択される少なくとも１つである、請求項４または５に記載のデータ運用方法。
【請求項７】
前記秘匿鍵は、複数のユーザに共通な識別情報である、請求項４または５に記載のデータ運用方法。
【請求項８】
前記秘匿鍵は、前記デジタルコンテンツの配布者固有の識別情報または前記デジタルコンテンツの著作者固有の識別情報のうちから選択される少なくとも１つである、請求項４または５に記載のデータ運用方法。
【請求項９】
コンテンツ管理者コンピュータがデジタルコンテンツに付加情報を可視的に配置してコンテンツ利用者コンピュータに配布するデータ運用方法であって、
配布されるデータは、前記付加情報が可視的に配置される位置を含む前記デジタルコンテンツの一部を部分データとして複製して暗号化した暗号化部分データ部と、前記デジタルコンテンツに前記付加情報を可視的に配置し、前記部分データ部の前記デジタルコンテンツにおける位置およびサイズに関する画像合成情報と前記暗号化部分データ作成時の暗号化に使用した暗号鍵の情報を含む許諾情報とを不可視情報として埋め込んだ許諾情報付きデータ部とを合成した合成データであり、
前記コンテンツ利用者コンピュータは、
配布された前記合成データから前記許諾情報付きデータ部と前記暗号化部分データ部とを分離する段階と、
分離された前記許諾情報付きデータ部から前記画像合成情報および前記許諾情報を抽出する段階と、
抽出された前記許諾情報を用いて、前記部分データ部作成時の暗号化に使用した前記暗号鍵を復元する段階と、
復元した前記暗号鍵を用いて前記暗号化部分データ部を前記部分データ部に復元する段階と、
前記許諾情報付きデータ部に、復元した前記部分データ部を前記画像合成情報に基づいて合成する段階と、
を実行するデータ運用方法。
【請求項１０】
前記許諾情報付きデータ部に埋め込まれる不可視情報には、ユーザが前記デジタルコンテンツを利用した利用回数情報を含み、ユーザが前記デジタルコンテンツを利用する毎に前記不可視情報を書き替える、請求項９に記載のデータ運用方法。

【請求項１１】
前記不可視情報に含まれる利用回数情報が所定値を超える場合にユーザによる利用を規制する、請求項１０に記載のデータ運用方法。
【請求項１２】
前記許諾情報付きデータ部から抽出された画像合成情報および許諾情報が保存されることを規制するように構成される、請求項９～１１のいずれかに記載のデータ運用方法。
【請求項１３】
前記許諾情報付きデータ部の画像データに、復元した部分データ部を合成した画像データが保存されることを規制するように構成される、請求項９～１２のいずれかに記載のデータ運用方法。
【請求項１４】
コンテンツ管理者コンピュータがデジタルコンテンツに付加情報を可視的に配置してコンテンツ利用者コンピュータに配布する際の前記コンテンツ管理者コンピュータに画像生成方法を実行させるプログラムを記録した記録媒体であって、
前記付加情報が可視的に配置される位置を含む前記デジタルコンテンツの一部を部分データ部として複製し、この部分データ部を暗号化して暗号化部分データ部を作成する段階と、
前記デジタルコンテンツに前記付加情報を可視的に配置して付加情報付きデータ部を作成する段階と、
前記部分データ部の前記デジタルコンテンツにおける位置およびサイズに関する画像合成情報と、前記暗号化部分データ部作成時の暗号化に使用した暗号鍵の情報を含む許諾情報とを、前記付加情報付きデータ部に不可視情報として埋め込んで許諾情報付きデータ部を作成する段階と、
前記暗号化部分データ部と前記許諾情報付きデータ部とを合成した合成データを作成する段階と、
を含む画像生成方法をコンピュータに実行せるプログラムを記録した記録媒体。
【請求項１５】
コンテンツ管理者コンピュータがデジタルコンテンツに付加情報を可視的に配置してコンテンツ利用者コンピュータに配布する際の前記コンテンツ利用者コンピュータに画像復元方法を実行させるプログラムを記録した記録媒体であって、
配布されるデータは、前記付加情報が可視的に配置される位置を含む前記デジタルコンテンツの一部を部分データとして複製して暗号化した暗号化部分データ部と、前記デジタルコンテンツに前記付加情報を可視的に配置し、前記部分データ部の前記デジタルコンテンツにおける位置およびサイズに関する画像合成情報と前記暗号化部分データ作成時の暗号化に使用した暗号鍵の情報を含む許諾情報とを不可視情報として埋め込んだ許諾情報付きデータ部とを合成した合成データであり、
配布された前記合成データから前記許諾情報付きデータ部と前記暗号化部分データ部とを分離する段階と、
分離された前記許諾情報付きデータ部から前記画像合成情報および前記許諾情報を抽出する段階と、
抽出された前記許諾情報を用いて、前記暗号化部分データ部作成時の暗号化に使用した前記暗号鍵を復元する段階と、
復元した前記暗号鍵を用いて前記暗号化部分データ部を前記部分データ部に復元する段階と、
前記許諾情報付きデータ部に、復元した前記部分データ部を前記画像合成情報に基づいて合成する段階と、
を含む画像復元方法をコンピュータ実行させるプログラムを記録した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】

本発明は、データ運用方法、画像生成方法のプログラムを記録する記録媒体、画像復元方法のプログラムを記録する記録媒体に関し、特に、付加情報が可視的に配置されたデジタルコンテンツを配布するデータ運用方法、配布する画像データをこのデータ運用方法で運用するための画像生成方法のプログラムを記録する記録媒体、配布される画像データを利用するための画像復元方法のプログラムを記録する記録媒体に関する。

【０００２】

【従来の技術】

コンピュータプログラムなどのソフトウェアや電子出版物では、光磁気ディスク（ＭＯ）、ディジタルビデオディスク（ＤＶＤ）、フロッピーディスク（ＦＤ）、ミニディスク（ＭＤ）、その他の記録媒体上に電子化データを格納して販売される。このような電子化データは、一般にコピーが容易であり、不正コピーが頻繁に行われている。このため、ソフトウェアベンダーや出版者側の著作権が侵害され著しく利益が阻害されるおそれがある。

【０００３】

また、インターネットやＣＡＴＶ、その他のネットワークなどを通じて配布される静止画像データ、動画像データを含む電子化データについても同様にして不正コピーが頻繁に行われ、著作権者の利益が損なわれている。

このような記録媒体上に格納された電子化データや各種ネットワークを通じて配布される電子化データなどのいわゆるデジタルコンテンツを保護するために、暗号鍵を用いてデジタルコンテンツを暗号化しこの暗号化された実データを配布することが行われる。

【０００４】

たとえば、ユーザが自分のパーソナルコンピュータからコンテンツの配布者側にアクセスを行い、デジタルコンテンツをハードディスク上にダウンロードを行ってこれを利用する場合を考える。まず、ユーザはホストコンピュータにアクセスしてダウンロードのためのプラグインモジュールを入手する。この後、使用しているハードディスクドライブの識別番号、使用しているコンピュータのＣＰＵ識別番号、その他ユーザ固有の識別情報をホストコンピュータ側に送付する。

【０００５】

コンテンツの配布者側では、デジタルコンテンツをコンテンツ鍵で暗号化した実データと、コンテンツ鍵をユーザ固有の識別情報で暗号化した許諾情報を、ユーザ側に送信する。

ユーザ側では、送られてきた暗号化実データと、許諾情報とを暗号化された状態のままハードディスクに記録する。デジタルコンテンツを利用する場合には、ハードディスクドライブの識別番号などのユーザ固有の識別情報を用いて、許諾情報を復号化し、コンテンツ鍵を取得する。このコンテンツ鍵を用いて、暗号化されたデジタルコンテンツを復号化してこれを利用する。

【０００６】

この場合、ユーザ個々にデジタルコンテンツの利用権を与える際に、デジタルコンテンツを暗号化するための暗号鍵を共通にすることができ、ユーザ毎に異なるユーザ固有の情報を用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。

上述の方法でデータの配布を行う場合、データ配布者は暗号化されたデジタルコンテンツと、暗号化されたデジタルコンテンツの復号鍵となる許諾情報とを別々に送付する必要がある。

【０００７】

また、ユーザ側においても、送付されてくる暗号化されたデジタルコンテンツとその許諾情報とを別々に記録媒体に格納しておく必要がある。

したがって、データ配布者側からユーザ側に送付される途中で許諾情報が破壊されたり、またはユーザ側の記録媒体上で許諾情報がなんらかの事故により破壊もしくは紛失した場合には、デジタルコンテンツを利用することができなくなり、再度許諾情報を入手する手順が必要となる。

【０００８】
　また、図書館の写本、美術館所蔵品などを写真やスキャナなどで画像データとして取り込み、これをユーザに利用させる場合、画像データが完全に暗号化されていると許諾情報のやりとりを行う前に、ユーザ側で所望の画像データを特定することが困難である。したがって、画像の一部がユーザ側で確認でき、かつ不正に流用されることがないように運用することが望ましい。
【０００９】
　このために、特開平8-241403号公報に示されるような、デジタルコンテンツに著作権情報などの付加情報を可視的な電子透かしとして埋め込んで配布することが考えられる。
【００１０】
【発明が解決しようとする課題】
　デジタルコンテンツに可視的な電子透かしとして付加情報を埋め込んで配布する場合、この付加情報を除去して元のデジタルコンテンツを復元するために、色度または輝度の変調データを画素毎に作成し、これを付加情報付きデジタルコンテンツと一緒に配布する必要があり、このようなデータの送受信に時間を要するとともに、データを格納するためのメモリ容量が大きく取られるという問題がある。
【００１１】
　本発明では、デジタルコンテンツの著作権や版権を損なうことなく、正規のユーザによる利用を容易にしたデータ運用方法、配布する画像データをこのデータ運用方法で運用するための画像生成方法のプログラムを記録する記録媒体、配布される画像データを利用するための画像復元方法のプログラムを記録する記録媒体を提供する。
【００１２】
【課題を解決するための手段】
　本発明に係るデータ運用方法は、コンテンツ管理者コンピュータがデジタルコンテンツに付加情報を可視的に配置してコンテンツ利用者コンピュータに配布するデータ運用方法であって、コンテンツ管理者コンピュータは、付加情報が可視的に配置される位置を含むデジタルコンテンツの一部を部分データ部として複製し、この部分データ部を暗号化して暗号化部分データ部を作成する段階と、デジタルコンテンツに付加情報を可視的に配置して付加情報付きデータ部を作成する段階と、部分データ部のデジタルコンテンツにおける位置およびサイズに関する画像合成情報と、暗号化部分データ部作成時の暗号化に使用した暗号鍵の情報を含む許諾情報とを、付加情報付きデータ部に不可視情報として埋め込んで許諾情報付きデータ部を作成する段階と、暗号化部分データ部と許諾情報付きデータ部とを合成した合成データを作成しこれを配布する段階とを実行する。
【００１３】
　ここで、付加情報は、可視的電子透かしとしてデジタルコンテンツに埋め込まれるものとすることができる。
　また、デジタルコンテンツに可視的電子透かしとして埋め込まれる付加情報と同等の付加情報を、部分データ部に不可視電子透かしとして埋め込み、これを暗号化して暗号化部分データ部を作成するように構成できる。
【００１４】
　さらに、画像合成情報および許諾情報は、秘匿鍵によって暗号化されて前記デジタルコンテンツに不可視情報として埋め込むように構成でき、この不可視情報をデジタルコンテンツの付加情報が配置される位置を含む部分に埋め込むことも可能である。このとき秘匿鍵は、ユーザ識別情報、ユーザ使用のコンピュータに搭載された機器の識別情報、ユーザ使用のコンピュータに搭載されたＣＰＵ識別情報、前記デジタルコンテンツを格納する記録媒体に固有の識別情報またはユーザ使用のコンピュータに登録されたユーザログイン情報のうちから選択される少なくとも１つとすることができ、また、複数のユーザに共通な識別情報とすることもでき、デジタルコンテンツの配布者固有の識別情報または前記デジタルコンテンツの著作者固有の識別情報のうちから選択される少なくとも１つとすることもできる。

【００１５】
また、配布された合成データから許諾情報付きデータ部と暗号化部分データ部とを分離する段階と、分離された許諾情報付きデータ部から画像合成情報および許諾情報を抽出する段階と、抽出された許諾情報を用いて、前記部分データ部を暗号化した暗号鍵を復元する段階と、復元した暗号鍵を用いて前記暗号化部分データ部を部分データ部に復元する段階と、前記許諾情報付きデータ部の画像データに、復元した部分データ部を前記画像合成情報に基づいて合成する段階とをさらに備える構成とすることができる。
【００１６】
ここでは、許諾情報付きデータ部に埋め込まれる不可視情報には、ユーザが前記デジタルコンテンツを利用した利用回数情報を含み、ユーザが前記デジタルコンテンツを利用する毎に前記不可視情報を書き替えるように構成できる。
また、不可視情報に含まれる利用回数情報が所定値を超える場合にユーザによる利用を規制するように構成できる。
【００１７】
さらに、許諾情報付きデータ部から抽出された画像合成情報および許諾情報が保存されることを規制するように構成でき、許諾情報付きデータ部の画像データに、復元した部分データ部を合成した画像データが保存されることを規制するように構成することもできる。
本発明では、コンテンツ管理者コンピュータがデジタルコンテンツに付加情報を可視的に配置してコンテンツ利用者コンピュータに配布するデータ運用方法であって、配布されるデータは、付加情報が可視的に配置される位置を含むデジタルコンテンツの一部を部分データとして複製して暗号化した暗号化部分データ部と、デジタルコンテンツに付加情報を可視的に配置し、部分データ部のデジタルコンテンツにおける位置およびサイズに関する画像合成情報と暗号化部分データ作成時の暗号化に使用した暗号鍵の情報を含む許諾情報とを不可視情報として埋め込んだ許諾情報付きデータ部とを合成した合成データであり、コンテンツ利用者コンピュータが、配布された合成データから許諾情報付きデータ部と暗号化部分データ部とを分離する段階と、分離された許諾情報付きデータ部から画像合成情報および許諾情報を抽出する段階と、抽出された許諾情報を用いて、部分データ部作成時の暗号化に使用した暗号鍵を復元する段階と、復元した暗号鍵を用いて暗号化部分データ部を部分データ部に復元する段階と、許諾情報付きデータ部に、復元した部分データ部を画像合成情報に基づいて合成する段階とを実行するデータ運用方法を提供する。
【００１８】
ここで、許諾情報付きデータ部に埋め込まれる不可視情報には、ユーザがデジタルコンテンツを利用した利用回数情報を含み、ユーザがデジタルコンテンツを利用する毎に不可視情報を書き替えるように構成できる。
また、不可視情報に含まれる利用回数情報が所定値を超える場合にユーザによる利用を規制するように構成できる。
【００１９】
さらに、許諾情報付きデータ部から抽出された画像合成情報および許諾情報が保存されることを規制するように構成できる。
また、許諾情報付きデータ部の画像データに、復元した部分データ部を合成した画像データが保存されることを規制するように構成することができる。
本発明では、コンテンツ管理者コンピュータがデジタルコンテンツに付加情報を可視的に配置してコンテンツ利用者コンピュータに配布する際のコンテンツ管理者コンピュータに画像生成方法を実行させるプログラムを記録した記録媒体であって、付加情報が可視的に配置される位置を含むデジタルコンテンツの一部を部分データ部として複製し、この部分データ部を暗号化して暗号化部分データ部を作成する段階と、デジタルコンテンツに付加情報を可視的に配置して付加情報付きデータ部を作成する段階と、部分データ部のデジタルコンテンツにおける位置およびサイズに関する画像合成情報と、暗号化部分データ部作成時の暗号化に使用した暗号鍵の情報を含む許諾情報とを、付加情報付きデータ部に不

可視情報として埋め込んで許諾情報付きデータ部を作成する段階と、暗号化部分データ部と許諾情報付きデータ部とを合成した合成データを作成する段階とを含む画像生成方法をコンピュータに実行せるプログラムを記録した記録媒体を構成する。ここで記録媒体とは、コンピュータが読み書き可能なフレキシブルディスク、ハードディスク、半導体メモリ、CD-ROM、ＤＶＤ、光磁気ディスク（ＭＯ）、その他のものが想定できる。

【００２０】

また、本発明では、コンテンツ管理者コンピュータがデジタルコンテンツに付加情報を可視的に配置してコンテンツ利用者コンピュータに配布する際のコンテンツ利用者コンピュータに画像復元方法を実行させるプログラムを記録した記録媒体であって、配布されるデータは、付加情報が可視的に配置される位置を含むデジタルコンテンツの一部を部分データとして複製して暗号化した暗号化部分データ部と、デジタルコンテンツに付加情報を可視的に配置し、部分データ部のデジタルコンテンツにおける位置およびサイズに関する画像合成情報と暗号化部分データ作成時の暗号化に使用した暗号鍵の情報を含む許諾情報とを不可視情報として埋め込んだ許諾情報付きデータ部とを合成した合成データであり、配布された合成データから許諾情報付きデータ部と暗号化部分データ部とを分離する段階と、分離された許諾情報付きデータ部から画像合成情報および許諾情報を抽出する段階と、抽出された許諾情報を用いて、暗号化部分データ部作成時の暗号化に使用した暗号鍵を復元する段階と、復元した暗号鍵を用いて暗号化部分データ部を部分データ部に復元する段階と、許諾情報付きデータ部に、復元した部分データ部を画像合成情報に基づいて合成する段階とを含む画像復元方法をコンピュータに実行させるプログラムを記録した記録媒体を構成する。

【００２１】

【発明の実施の形態】

〔発明の概要〕

図１に本発明の概要構成を示す。

デジタルコンテンツの著作者、版権者などであるデジタルコンテンツ提供者が扱うコンピュータ（以下、コンテンツ提供者１と称す）は、運用を行うデジタルコンテンツ１１の管理者が扱うコンピュータ（以下、コンテンツ管理者２と称す）に提供する。

【００２２】

コンテンツ管理者２は、コンテンツ提供者１から提供されるデジタルコンテンツ１１と、このデジタルコンテンツ１１を運用する際に用いる暗号鍵およびこのデジタルコンテンツ１１を利用するユーザの利用者情報を管理する。

コンテンツの利用者が扱うコンピュータ（以下、コンテンツ利用者３と称す）は、コンテンツ管理者２が管理しているデジタルコンテンツを利用したい場合には、利用者情報１４をコンテンツ管理者２に送信する。

【００２３】

コンテンツ管理者２は、コンテンツ利用者３から送信された利用者情報１４を管理するとともに、この利用者情報１４に基づくコンテンツ使用許諾情報１３を作成し、このコンテンツ使用許諾情報１３とデジタルコンテンツ１１とを含む配布用データ１２に加工してコンテンツ利用者３に送信する。

コンテンツ管理者２は、デジタルコンテンツ１１の一部を部分データ部としてコピーしてこれを暗号化する。デジタルコンテンツ１１の部分データ部に対応する位置に、著作権情報などの付加情報を可視的なウォーターマークとして埋め込む。利用者情報１４を用いて、部分データ部の位置やサイズを示す画像合成情報と、部分データ部を暗号化する際に用いた暗号鍵の情報とを暗号化して使用許諾情報１３を作成する。この使用許諾情報１３をデジタルコンテンツ１１中に不可視なウォーターマークとして埋め込み、暗号化された部分データ部と合成して配布用データ１２とする。

【００２４】

このとき、コンテンツ提供者１とコンテンツ管理者２は同一であってもよい。

〔コンテンツ管理者〕

コンテンツ管理者２側の概略構成を示す機能ブロック図を図２に示す。

コンテンツ管理者２は、データ運用を行うためのホストコンピュータおよびサーバアプリケーションで構成されており、コンテンツを管理するコンテンツ管理部２１、著作権情報などの付加情報の入力および付加情報の埋め込み位置などを決定するための付加情報入力部２２、デジタルコンテンツの一部を複製したり、原画像に付加情報を可視的に埋め込む機能を有する画像加工部２３、デジタルコンテンツから複製される部分データ部をコンテンツ鍵で暗号化する画像暗号化部２４、コンテンツ鍵に関する情報および部分データ部の位置とサイズを示す画像合成情報を暗号化して許諾情報を作成する許諾情報作成部２５、コンテンツ鍵の情報および画像合成情報を不可視情報としてデジタルコンテンツに埋め込む情報埋め込み部２６、部分データ部を暗号化するためのコンテンツ鍵を管理するコンテンツ鍵管理部２７、コンテンツ利用者３の利用者情報を取得してこれを管理する利用者情報取得部２８などを含んでいる。

【００２５】

〔コンテンツ利用者〕

コンテンツ利用者３側の概略構成を示す機能ブロック図を図３に示す。

コンテンツ利用者３は、パーソナルコンピュータやワークステーションなどの端末機とコンテンツを利用するためのアプリケーションで構成されており、使用しているハードディスクドライブの識別番号、コンピュータに搭載されているＣＰＵの識別番号、その他の利用者固有の識別情報を管理する利用者情報管理部３１、コンテンツ管理者２からの配布データを取得する配布データ取得部３２、配布データから画像合成情報を抽出するための画像合成情報取得部３３、配布データからコンテンツ鍵の情報を取得するコンテンツ鍵取得部３４、配布データのうち暗号化された部分データ部を復号化する画像復号化部３５、復号化された部分データ部をデジタルコンテンツに合成する画像加工部３６、利用者情報およびコンテンツの利用状況に基づく利用情報を管理する利用情報管理部３７、復元されたデジタルコンテンツを表示するなどのデジタルコンテンツを動作させるコンテンツ動作部３８を備えている。

【００２６】

〔コンテンツ配布〕

デジタルコンテンツを配布する際に、コンテンツ管理者２側が行う動作を図４および図５に基づいて説明する。

ステップ１１では、配布を行うデジタルコンテンツ１１に関するコンテンツ情報４１が入力されたか否かを判別する。コンテンツ情報４１は、デジタルコンテンツ１１の著作権者に関する情報や配布を行う管理者情報などであり、デジタルコンテンツ１１に可視的なウォーターマークとして埋め込むためのものである。このコンテンツ情報４１は、キーボードやその他の入力手段によりオペレータにより入力されるか、あるいはデジタルコンテンツを管理するデータベースファイルなどから対応するものを抽出することによって取得することができる。

【００２７】

ステップＳ１１において、コンテンツ情報４１の入力があったと判断した場合、ステップＳ１２に移行する。ステップＳ１２では、入力されたコンテンツ情報４１を記憶手段に格納して管理する。

ステップＳ１３では、コンテンツ情報４１を可視的なウォーターマークとして埋め込む位置およびサイズに関する画像合成情報４２の入力があったか否かを判別する。

【００２８】

たとえば、キーボードやその他の入力手段によりオペレータにより、始点座標Ｐ（ｘ，ｙ）および画素数Ｇ（ｘ，ｙ）が入力された場合に、これらを画像合成情報４２の入力とみなしてステップＳ１４に移行する。また、アプリケーションで設定される始点座標Ｐ（ｘ，ｙ）および画素数Ｇ（ｘ，ｙ）などの画像合成情報４２が存在する場合にも、画像合成情報４２の入力があったとみなしてステップＳ１４に移行する。ステップＳ１４では、入力された画像合成情報４２を記憶手段に格納して管理する。

【００２９】
ステップＳ１５では、画像合成情報４２に基づいてデジタルコンテンツ１１の一部を複製して、部分データ部４３を作成する。これと同時に、部分データ部４３の対応するデジタルコンテンツ１１の位置に、コンテンツ情報４１を可視的なウォーターマークとして埋め込む。コンテンツ情報４１を可視的に埋め込む方法としては、色度変調を伴う方法、輝度変調を伴う方法などを用いることが可能である。
【００３０】
ステップＳ１６では、コンテンツ情報４１を不可視なウォーターマークとして部分データ部４３に埋め込んで、付加情報付き部分データ部４４を作成する。部分データ部４３の特定の周波数帯域にコンテンツ情報４１を挿入するか、あるいはデータの一部を間引きしてここにコンテンツ情報４１を挿入するように構成することによって、不可視なウォーターマークとして情報を付加することができる。
【００３１】
ステップＳ１７では、付加情報付き部分データ部４４をコンテンツ鍵４５で暗号化して暗号化部分データ部４６とする。コンテンツ鍵４５は、コンテンツ管理者２側で管理されるものであって、暗号化および復号化が同一の共通鍵とすることができる。
ステップＳ１８では、画像合成情報４２とコンテンツ鍵４５とを秘匿鍵４７で暗号化して許諾情報４８を作成する。秘匿鍵４７は、コンテンツ利用者３側から送信される利用者情報１４に基づいて作成される暗号鍵である。利用者情報１４は、予めコンテンツ利用者３側から送信されてくるものであり、ユーザのＩＤ番号やパスワードなどのユーザ識別情報、ユーザ使用のコンピュータに搭載された機器の識別情報、ユーザ使用のコンピュータに搭載されたＣＰＵ識別情報、デジタルコンテンツを格納する記録媒体に固有の識別情報またはユーザ使用のコンピュータに登録されたユーザログイン情報の少なくとも１つを用いることができる。
【００３２】
ステップＳ１９では、付加情報付きデータ部４９の部分データ部４３が対応する以外の位置に、許諾情報４８を不可視なウォーターマークとして埋め込んで、許諾情報付きデータ部５０を作成する。
ステップＳ２０では、許諾情報付きデータ部５０と暗号化部分データ部４６とを一体化して合成データ６０を作成する。このようにして得られる合成データ６０は、コンテンツ利用者３の要望を応じて、インターネットなどのオンラインネットワークやCD-ROM、DVDその他の記録媒体などを介して配布される。
【００３３】
〔コンテンツ利用〕
コンテンツ利用者３が配布されたデジタルコンテンツを利用する場合の動作を図６、図７に基づいて説明する。
ステップＳ３１では、コンテンツ管理者２から合成データ６０を取得する。このとき、コンテンツ利用者３は、予めコンテンツ管理者２側にアクセスを行い、コンテンツ管理者２が管理しているデジタルコンテンツを利用したい旨を伝え、利用者固有の利用者情報１４をコンテンツ管理者２側に送っているものとする。合成データ６０は、各種ネットワークを通じてダウンロードすることで取得する形態、コンテンツ管理者２から記録媒体に記録された状態で配布される形態のいずれの方法でも取得することができる。取得した合成データ６０は、コンテンツ利用者３が使用しているハードディスク、その他の記録媒体上に格納される。
【００３４】
ステップＳ３２では、暗号化データ部６１と許諾情報付きデータ部６２とを分離する。このとき、許諾情報付きデータ部６２は、許諾情報が不可視のウォーターマークとして埋め込まれ、著作権情報などを示すコンテンツ情報が可視的ウォーターマークとして埋め込まれている。ステップＳ３３では、許諾情報付きデータ部６２を表示させる。表示される許諾情報付きデータ部６２は、元のデジタルコンテンツに著作権情報などを示すコンテン

ツ情報が可視的に埋め込まれたものであり、コンテンツ情報が埋め込まれている部分以外の位置では、元のデジタルコンテンツが確認できるように構成されている。

【００３５】

ステップＳ３４では、コンテンツ利用者３による利用要求があったか否かを判別する。許諾情報付きデータ部６２の表示において、コンテンツ利用者３がこれを利用する旨の指示を行った場合には、ステップＳ３５に移行する。

ステップＳ３５では、許諾情報付きデータ部６２から許諾情報６３を抽出する。許諾情報付きデータ部６２に不可視なウォーターマークとして埋め込まれている許諾情報６３は、周波数解析または画像解析を行うことによって抽出することができる。

【００３６】

ステップＳ３６では、許諾情報６３を復号化してコンテンツ鍵６４と画像合成情報６５とを取り出す。許諾情報６３は、利用者情報１４に基づく秘匿鍵４７で暗号化されている。このため、ユーザのＩＤ番号やパスワードなどのユーザ識別情報、ユーザ使用のコンピュータに搭載された機器の識別情報、ユーザ使用のコンピュータに搭載されたＣＰＵ識別情報、デジタルコンテンツを格納する記録媒体に固有の識別情報またはユーザ使用のコンピュータに登録されたユーザログイン情報などの利用者情報１４に基づいて秘匿鍵４７に対応する復号鍵６６を作成し、この復号鍵６６を用いて許諾情報６３を復号化することによって、コンテンツ鍵６４と画像合成情報６５とを取り出すことが可能となる。

【００３７】

ステップＳ３７では、取り出したコンテンツ鍵６４を用いて、暗号化部分データ部６１を復号化し、部分データ部６７を復元する。

ステップＳ３８では、画像合成情報６５に含まれる部分データ部６７の位置およびサイズに関する情報に基づいて、許諾情報付きデータ部６２の所定位置のデータを部分データ部６７に置き換えて、元のデジタルコンテンツ６８を復元する。

【００３８】

ステップＳ３９では、復元されたデジタルコンテンツ６３をディスプレイ上に表示させるなどしてコンテンツの動作を行う。置き換えられた部分データ部６７には、著作権情報などのコンテンツ情報が不可視のウォーターマークとして埋め込まれているため、復元されたデジタルコンテンツ６８は不可視情報としてコンテンツ情報が埋め込まれたものとなっており、表示されるデジタルコンテンツ６３は、不可視のウォーターマークとしてコンテンツ情報を含むものとなっている。

【００３９】

〔許諾情報の構造〕

Ａ）デジタルコンテンツ１１中に不可視なウォーターマークとして埋め込まれる許諾情報の構造を図８に示す。

許諾情報データ７０は、暗号化に用いた秘匿鍵の種別が格納される秘匿鍵種別領域７１と、その秘匿鍵によって暗号化された後の情報が格納される秘匿鍵情報領域７２とで構成される。

【００４０】

秘匿鍵種別領域７１に格納される秘匿鍵種別は、利用者情報１４のうちのどのような情報を秘匿鍵として用いたかを示すものである。たとえば、ユーザがデータを格納する光磁気ディスク（ＭＯ）の媒体ＩＤを秘匿鍵とする場合に、秘匿鍵種別領域７１に格納する値を”０”とし、ユーザが設定したパスワードを秘匿鍵とする場合に、秘匿鍵種別領域７１に格納する値を”１”とするなどの設定を予め定めておく。

【００４１】

秘匿鍵情報領域７２は、画素位置領域７３，Ｘ画素サイズ領域７４，Ｙ画素サイズ領域７５，コンテンツ鍵領域７６で構成される。画像位置領域７３は、部分データ部４３を複製する際の始点座標Ｐ（ｘ，ｙ）を格納するものである。この始点座標Ｐ（ｘ，ｙ）は、たとえば部分データ部４３の左上隅の点の座標を示すものであり、コンテンツ管理者２が配布データを作成する際に入力されるものである。

【００４２】
Ｘ画素サイズ領域７４およびＹ画素サイズ領域７５には、それぞれ部分データ部４３のｘ方向の画素数Ｇ（ｘ）およびｙ方向の画素数Ｇ（ｙ）が格納される。このｘ方向およびｙ方向の画素数Ｇ（ｘ，ｙ）は、始点座標Ｐ（ｘ，ｙ）と同様にコンテンツ管理者２が配布データを作成する際に入力されるものである。
コンテンツ鍵領域７６には、コンテンツ管理者２側で管理しているコンテンツ鍵４５が格納される。秘匿鍵情報領域７２の画素位置領域７３，Ｘ画素サイズ領域７４，Ｙ画素サイズ領域７５，コンテンツ鍵領域７６に格納されるデータは、それぞれ秘匿鍵種別領域７１のデータで特定される秘匿鍵で暗号化されている。
【００４３】
Ｂ）デジタルコンテンツ１１中に不可視なウォーターマークとして埋め込まれる許諾情報の構造は、図９に示すような構造とすることができる。
この場合、許諾情報データ８０は、画素位置領域８１，Ｘ画素サイズ領域８２，Ｙ画素サイズ領域８３，秘匿鍵種別領域８４，秘匿鍵情報領域８５で構成される。画素位置領域８１，Ｘ画素サイズ領域８２，Ｙ画素サイズ領域８３は、それぞれ部分データ部４３を複製する際の始点座標Ｐ（ｘ，ｙ）、部分データ部４３のｘ方向の画素数Ｇ（ｘ）およびｙ方向の画素数Ｇ（ｙ）を格納する。これら画素位置領域８１，Ｘ画素サイズ領域８２，Ｙ画素サイズ領域８３に格納されるデータは、前述と同様にしてコンテンツ管理者２側で配布データを作成する際に入力されるものであり、暗号化されずに格納される。
【００４４】
秘匿鍵種別領域８４は、利用者情報１４のうちのどのような情報を秘匿鍵として用いたかを示す秘匿鍵種別情報を格納するものであり、たとえば、前述と同様に、ユーザがデータを格納する光磁気ディスク（ＭＯ）の媒体ＩＤを秘匿鍵とする場合に”０”、ユーザが設定したパスワードを秘匿鍵とする場合に”１”が格納される。
【００４５】
秘匿鍵情報領域８５は、コンテンツ鍵４５を秘匿鍵で４７で暗号化した後の情報を格納する。
〔アクセス制限方法〕
配布されたデータがコンテンツ利用者３側において復元される過程で、復号化されたコンテンツ鍵６４、コンテンツ鍵６４で復号化された部分データ部６７および復元されたデジタルコンテンツ６８が、メモリ内に保存されたり記憶媒体上に保存されることを許容すると、保存されたデータを用いて不正なデータ配布が行われるおそれがある。これを防止するためのアクセス制限方法を図１０に基づいて説明する。
【００４６】
配布されたデータをコンテンツ利用者３側で利用するためのアプリケーションは、モニタ機能を備えており、コンテンツ利用プログラムの起動時にステップＳ４１において、モニタ機能プログラムを起動させる。
このモニタ機能プログラムは、コンテンツ利用プログラムの構成要素である複数のライブラリ間でのデータの授受を横取りする機能を持つ不正プログラム（メモリフックコマンド：Application Programming Interface）を監視する。モニタ機能プログラムによりメモリフックコマンドの発生を検出した場合、プログラムの利用を制限するように構成される。
【００４７】
ステップＳ４３では、メモリフックに関連するコマンドによるプロセスが起動したか否かを判別する。メモリフック関連のコマンドを実行させるようなプロセスが起動した場合にはステップＳ４４に移行し、なかった場合にはステップＳ４５に移行する。
ステップＳ４４では、エラー処理を実行する。このエラー処理では、メモリフックコマンドに基づく不正プログラムが起動した旨のエラー表示を行い、ステップＳ４７に移行する。
【００４８】

ステップＳ４５では、デジタルコンテンツを利用するためのアプリケーションによる処理を実行する。ステップＳ４６では、このアプリケーションの終了を行うか否かを判別する。ユーザにより終了指示がなされた場合には、ステップＳ４７に移行する。

ステップＳ４７では、コンテンツ利用のためのアプリケーションを終了する。

【００４９】

このように構成することによって、プログラムが実行中にメモリに書き込まれるデータの横取りを制限し、配布されたデータから得られるコンテンツ鍵６４、デジタルコンテンツ６８などが不正に保存されることを防止できる。

〔他の実施形態〕

（Ａ）デジタルコンテンツ１１の部分データ部４３に対応する位置に、全く異なる画像を合成して付加情報付きデータ部４９を構成することも可能である。この場合、合成する画像はコンテンツ情報４１を含むものであっても良く、またコンテンツ情報４１を含まない画像を合成することも可能である。

（Ｂ）デジタルコンテンツ１１の部分データ部４３に対応する位置に、コンテンツ情報４１を可視的なウォーターマークとして埋め込んだ後、暗号化された許諾情報４８を不可視なウォーターマークとして埋め込んで、許諾情報付きデータ部５０を作成してもよい。

（Ｃ）許諾情報６３を復号化するための復号鍵６６は、暗号化された許諾情報４８を作成する際に用いた秘匿鍵４７と共通とすることができる。

【００５０】

また、暗号化された許諾情報４８を作成する際に用いる秘匿鍵４７を秘密鍵とし、コンテンツ利用者３が予めコンテンツ管理者２から提供された公開鍵を復号鍵６６とすることも可能である。

（Ｄ）コンテンツ利用者３がデジタルコンテンツを利用した利用回数を、デジタルコンテンツ６８に埋め込まれた不可視なウォーターマークとして備える構成とすることができる。この場合、許諾情報付きデータ６２に不可視なウォーターマークとして埋め込まれている許諾情報６３とともに利用回数の情報をウォーターマークとして埋め込む構成とすることができ、コンテンツ利用者３がこのデジタルコンテンツを利用する毎に不可視なウォーターマークを書き替えるように構成する。

【００５１】

コンテンツ利用者３によりデジタルコンテンツを利用する旨の指示がなされた時、利用回数が所定数を超えている場合にはこのデジタルコンテンツの利用を制限するように構成することが可能である。

また、利用回数が所定回数を超えた場合に、不可視ウォーターマークとして埋め込まれている許諾情報を書き替えて、それ以降の利用を制限するように構成することも可能である。

（Ｅ）上述したような本発明のプログラムを記録した記録媒体は本発明に含まれる。ここで記録媒体とは、コンピュータが読み書き可能なフロッピーディスク、ハードディスク、半導体メモリ、CD-ROM、ＤＶＤ、光磁気ディスク（ＭＯ）、その他のものが想定できる。

（Ｆ）また、上述したような本発明のプログラムを伝送する伝送媒体についても本発明に含まれる。ここで伝送媒体とは、プログラム情報を搬送波として伝搬させて供給するためのコンピュータネットワーク（ＬＡＮ、インターネット、無線通信ネットワーク）システムにおける通信媒体（光ファイバ、無線回線、その他）を含む。

【００５２】

【発明の効果】

本発明によれば、デジタルコンテンツに付加情報を可視的に配置し、付加情報が配置される位置を含む部分データ部を暗号化する際の暗号鍵の情報と画像合成情報とを含む許諾情報を不可視情報として埋め込み、暗号化された部分データ部とともに配布するため、暗号化部分データ部を復号化する際の復号鍵を別ルートで配送する必要がなく、コンテンツ利用者はデジタルコンテンツの概要を容易に確認できるとともに、正規の利用者は配布されてきた合成データから容易に元のデジタルコンテンツを復元して利用することが可能と

なる。

【図面の簡単な説明】

【図１】　本発明の概略構成図。

【図２】　コンテンツ管理者側の概略構成図。

【図３】　コンテンツ利用者側の概略構成図。

【図４】　配布データ作成時のフローチャート。

【図５】　配布データ作成時の原理図。

【図６】　コンテンツ利用時のフローチャート。

【図７】　コンテンツ利用時の原理図。

【図８】　許諾情報の構造の一例を示す説明図。

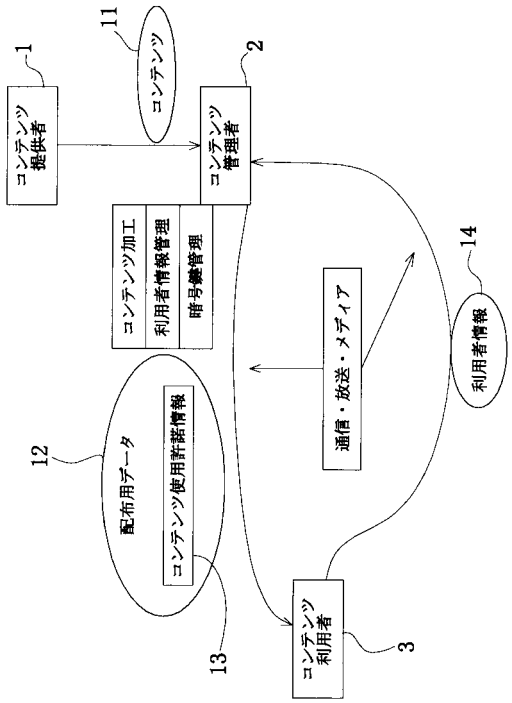
【図９】　許諾情報の構造の他の例を示す説明図。

【図１０】　アクセス制御方法の一例を示すフローチャート。

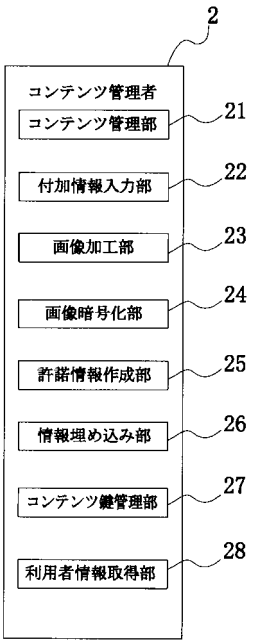
【符号の説明】

１　　コンテンツ提供者
２　　コンテンツ管理者
３　　コンテンツ利用者
１１　　デジタルコンテンツ
１４　　利用者情報
４１　　コンテンツ情報
４２　　画像合成情報
４３　　部分データ部
４５　　コンテンツ鍵
４６　　暗号化部分データ部
４７　　秘匿鍵
４８　　許諾情報
４９　　付加情報付きデータ部
５０　　許諾情報付きデータ部
６０　　合成データ
６１　　暗号化部分データ部
６２　　許諾情報付きデータ部
６３　　許諾情報
６４　　コンテンツ鍵
６５　　画像合成情報
６６　　復号鍵
６７　　部分データ部
６８　　デジタルコンテンツ

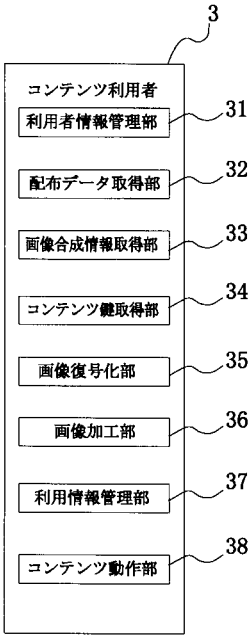
【図１】


1
コンテンツ提供者
11
コンテンツ
2
コンテンツ管理者
コンテンツ加工
利用者情報管理
暗号鍵管理
14
利用者情報
通信・放送・メディア
12
配布用データ
コンテンツ使用許諾情報
13
コンテンツ利用者
3

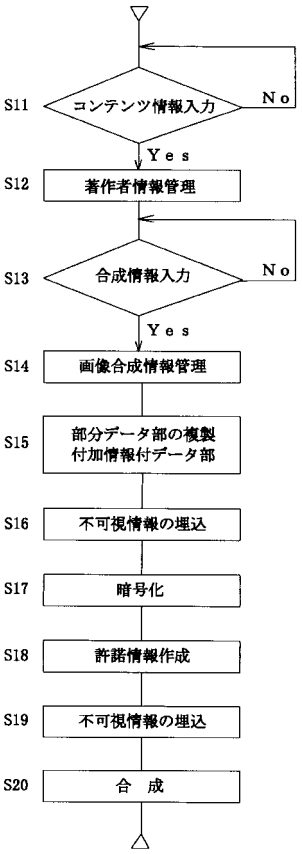
【図２】


2
コンテンツ管理者
コンテンツ管理部
21
付加情報入力部
22
画像加工部
23
画像暗号化部
24
許諾情報作成部
25
情報埋め込み部
26
コンテンツ鍵管理部
27
利用者情報取得部
28

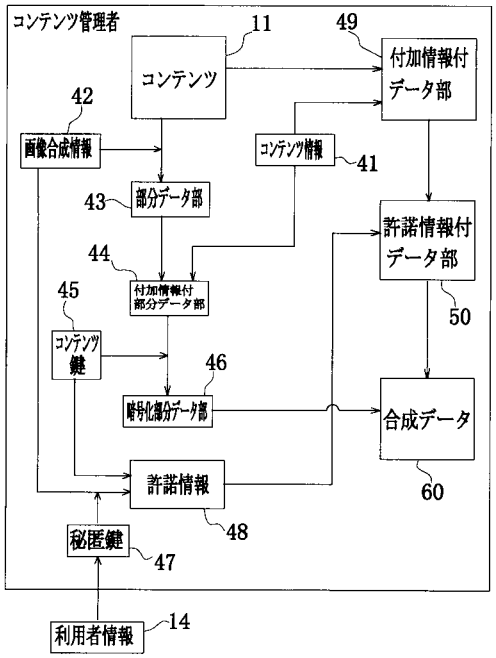
【図３】


3
コンテンツ利用者
利用者情報管理部
31
配布データ取得部
32
画像合成情報取得部
33
コンテンツ鍵取得部
34
画像復号化部
35
画像加工部
36
利用情報管理部
37
コンテンツ動作部
38

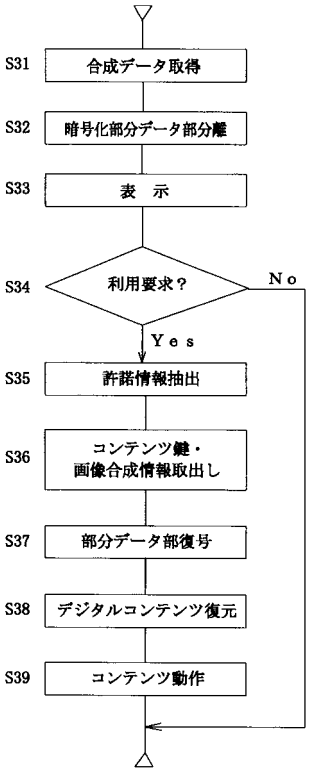
【図４】


S11
コンテンツ情報入力
No
Yes
S12
著作者情報管理
S13
合成情報入力
No
Yes
S14
画像合成情報管理
S15
部分データ部の複製
付加情報付データ部
S16
不可視情報の埋込
S17
暗号化
S18
許諾情報作成
S19
不可視情報の埋込
S20
合　成

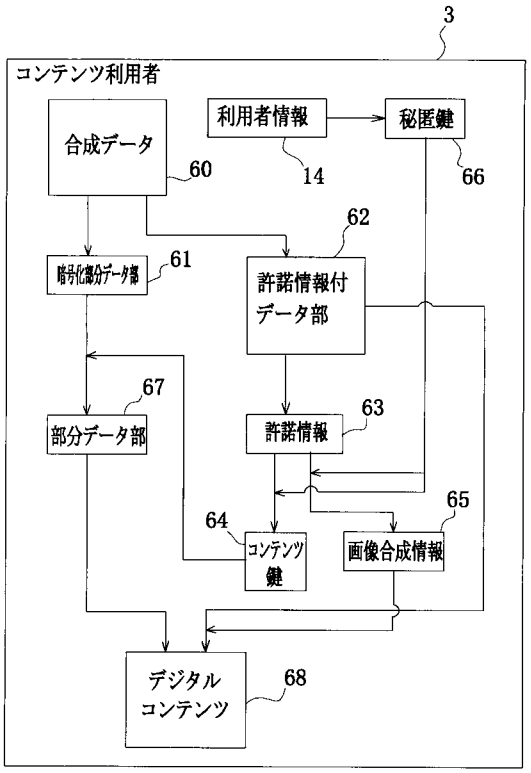
【図５】


コンテンツ管理者
11
49
コンテンツ
付加情報付データ部
42
画像合成情報
コンテンツ情報
41
43
部分データ部
許諾情報付データ部
44
付加情報付部分データ部
45
コンテンツ鍵
50
46
暗号化部分データ部
合成データ
60
許諾情報
48
秘匿鍵
47
利用者情報
14

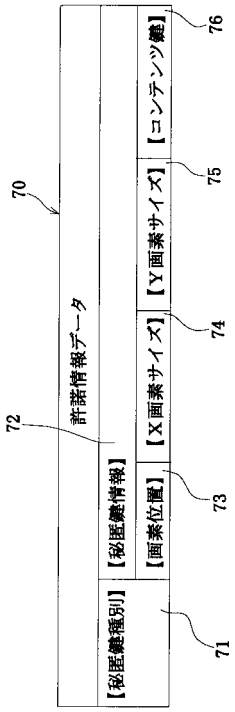
【図６】


S31
合成データ取得
S32
暗号化部分データ部分離
S33
表　示
S34
利用要求？
No
Yes
S35
許諾情報抽出
S36
コンテンツ鍵・画像合成情報取出し
S37
部分データ部復号
S38
デジタルコンテンツ復元
S39
コンテンツ動作

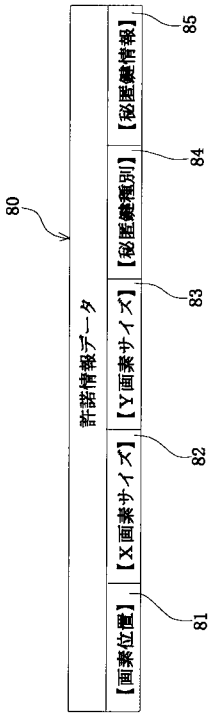
【図７】


3
コンテンツ利用者
合成データ
60
利用者情報
14
秘匿鍵
66
62
暗号化部分データ部
61
許諾情報付データ部
67
部分データ部
63
許諾情報
65
64
コンテンツ鍵
画像合成情報
デジタルコンテンツ
68

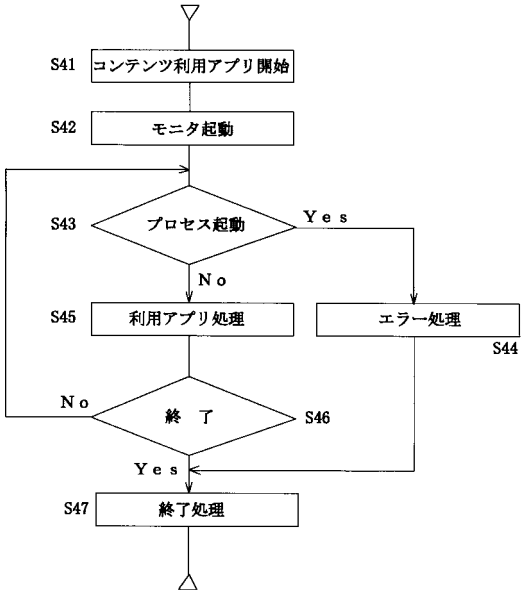
【図８】


70
許諾情報データ
72
【秘匿鍵種別】
【秘匿鍵情報】
【画素位置】
【X画素サイズ】
【Y画素サイズ】
【コンテンツ鍵】
71
73
74
75
76

【図９】


80
許諾情報データ
【画素位置】
【X画素サイズ】
【Y画素サイズ】
【秘匿鍵種別】
【秘匿鍵情報】
81
82
83
84
85

【図１０】


S41
コンテンツ利用アプリ開始
S42
モニタ起動
S43
プロセス起動
Yes
No
S45
利用アプリ処理
エラー処理
S44
No
終 了
S46
Yes
S47
終了処理

フロントページの続き

(51)Int.Cl.　　F I
H04N　7/081　(2006.01)

(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　橋本　晋二
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　村本　一彦
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　高橋　克

(56)参考文献　特開平１１－２８３３２７（ＪＰ，Ａ）
特開平１１－１３６６１８（ＪＰ，Ａ）
特開平１１－２８９２５５（ＪＰ，Ａ）
特開平１１－３４４９２６（ＪＰ，Ａ）
特開２００１－０５１９６０（ＪＰ，Ａ）
森本　典繁，“電子透かし技術”，電子情報通信学会誌，社団法人電子情報通信学会，１９９９年　8月２５日，第８２巻，第８号，第８３６－８３８頁

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 12/14
G06F　9/06
G06F 15/00
G06F 17/60
G11B 20/10
H04N　1/387
H04N　5/00
H04N　7/08
H04N　7/081
H04N　7/167