(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-40780
(P2004-40780A)
(43)公開日　平成16年2月5日(2004.2.5)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04N 7/167	H04N	7/167	Z	5C064
H04L 9/18	H04L	9/00	651	5J104

審査請求 未請求　請求項の数 24　ＯＬ　外国語出願　（全 37 頁）

(21)出願番号　特願2003-143298(P2003-143298)
(22)出願日　平成15年5月21日(2003.5.21)
(31)優先権主張番号　0206405
(32)優先日　平成14年5月24日(2002.5.24)
(33)優先権主張国　フランス(FR)

(71)出願人　591034154
フランス　テレコム
ＦＲＡＮＣＥ　ＴＥＬＥＣＯＭ
フランス国、７５０１５　パリ、プラス・ダルレ、６
(74)代理人　100062007
弁理士　川口　義雄
(74)代理人　100113332
弁理士　一入　章夫
(74)代理人　100114188
弁理士　小野　誠
(74)代理人　100103920
弁理士　大崎　勝真
(74)代理人　100124855
弁理士　坪倉　道明

最終頁に続く

(54)【発明の名称】ビデオ信号にスクランブルをかけ、スクランブルを解除する方法と、この方法を実施するためのシステム、符号化器、復号化器、一斉送信サーバ、および、データ媒体

(57)【要約】
【課題】ビデオコンテンツのスクランブル化を可能にする一方、コンテンツがある程度は可視のままであることを確実にするビデオ信号のスクランブル解除法を提供すること。
【解決手段】本発明は、特に視聴覚情報へのアクセスを制御するために、暗号化キーK_Tを使用してビデオ信号Ｓにスクランブルをかける方法に関する。ビデオ信号は、暗号化キーから導出されるマーキングキー３６を使用することによってビデオ信号にタトゥーイング関数を適用すること（３８）によってスクランブルがかけられ、タトゥーイング関数は、ビデオ信号におけるタトゥーイングの可視性の調整を可能にするために、タトゥーイングの振幅を調節するためのパラメータを含む。本発明は、双対のスクランブル解除方法、および、前記方法を実施するためのシステム、符号化器、復号化器、一斉送信サーバ、および、データ媒体も提供する。
【選択図】　図２

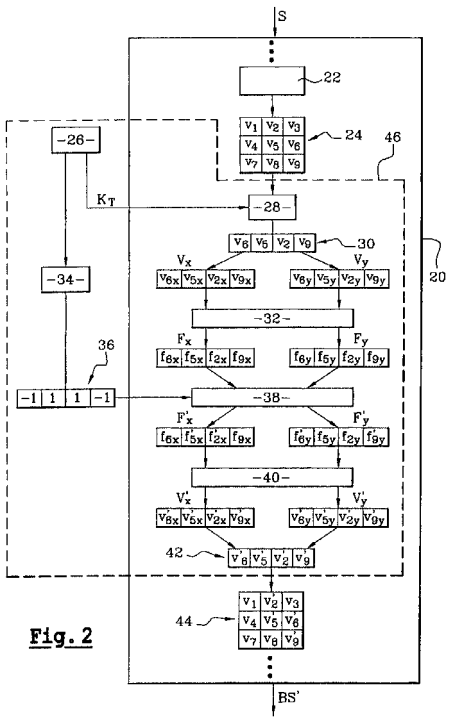

Fig. 2

【特許請求の範囲】
【請求項１】
視聴覚情報へのアクセスを制御するために暗号化キー（K_T）を使用して、ビデオ信号（Ｓ）にスクランブルをかける方法であって、前記暗号化キーから導出されるマーキングキー（３６）を使用して、前記ビデオ信号にタトゥーイング関数を適用すること（３８）によって前記ビデオ信号にスクランブルをかけ、前記タトゥーイング関数が、前記ビデオ信号におけるタトゥーイングの可視性の調整を可能にするタトゥーイングの振幅を調節するためのパラメータを含むことを特徴とするスクランブルをかける方法。
【請求項２】
前記視聴覚信号が、一斉送信サーバ（１０）からアクセス可能であることを特徴とする請求項１に記載のスクランブルをかける方法。
【請求項３】
前記視聴覚信号が、読み出しのためにアクセス可能であるデータ媒体（１２）に保存されることを特徴とする請求項１または２に記載のスクランブルをかける方法。
【請求項４】
前記タトゥーイング関数が、前記ビデオ信号（Ｓ）を符号化すること（２０）によって得られる動きベクトル（V_6，V_5，V_2，V_9）に適用されることを特徴とする請求項１から３のいずれか一項に記載のスクランブルをかける方法。
【請求項５】
前記タトゥーイング関数が、前記動きベクトルの周波数表示（F_x，F_y）に適用されることを特徴とする請求項４に記載のスクランブルをかける方法。
【請求項６】
前記スクランブルをかけることが、
前記ビデオ信号を符号化することによって得られる動きベクトルのセット（２４）から動きベクトル（V_6，V_5，V_2，V_9）を選択する（２８）ステップと、
前記選択されたベクトルの横軸成分および縦軸成分を、それぞれ横軸ベクトル（V_x）および縦軸ベクトル（V_y）と呼ぶ２つのベクトルに分離するステップと、
一次元ＤＣＴ型変換を前記２つのベクトルの各々に適用する（３２）ステップと、
前記マーキングキー（３６）を使用して、前記タトゥーイング関数を前記横軸ベクトルおよび前記縦軸ベクトルのＤＣＴ変換の成分（F_x，F_y）に適用する（３８）ステップと、
タトゥーイングの後に、前記選択された動きベクトルに対して新しい値を提供するために、前記横軸ベクトルおよび前記縦軸ベクトルに逆ＤＣＴ変換を行い、それらのベクトルを再結合させるステップを含むことを特徴とする請求項５に記載のスクランブルをかける方法。
【請求項７】
前記動きベクトル（V_6，V_5，V_2，V_9）が、符号化されたビデオストリーム（ＢＳ）から直接抽出され、符号化された後に前記ビデオ信号にスクランブルをかける（４６）ことを特徴とする請求項４から６のいずれか一項に記載のスクランブルをかける方法。
【請求項８】
前記ビデオ信号を符号化する（２０）の間に前記動きベクトル（V_6，V_5，V_2，V_9）が選択され、前記ビデオ信号が符号化される間に前記ビデオ信号にスクランブルをかける（４６）ことを特徴とする請求項４から６のいずれか一項に記載のスクランブルをかける方法。
【請求項９】
前記スクランブルをかけることが、オーサの権利に関する情報を含むタトゥーイングキーを使用してタトゥーイング関数を適用することによって、前記ビデオ信号（Ｓ）の不可視タトゥーイングに組み合されることを特徴とする請求項１から８のいずれか一項に記載のスクランブルをかける方法。
【請求項１０】

前記オーサの権利の情報がビデオの識別子（ＵＩＤ）を含み、オーサの識別子が前記ビデオに対する権利を有することを特徴とする請求項９に記載のスクランブルをかける方法。
【請求項１１】
前記ビデオ信号（Ｓ）にスクランブルをかけるために、前記マーキングキー（３６）の代わりに使用される新しいマーキングキーを生成するための一対一対応を提供する関数を使用して、前記タトゥーイングキーがマーキングキー（３６）に結合されることを特徴とする請求項９または１０に記載のスクランブルをかける方法。
【請求項１２】
前記ビデオ信号（Ｓ）が、ＭＰＥＧ－２またはＭＰＥＧ－４に準拠して符号化（２０）されることを特徴とする請求項１から１１のいずれか一項に記載のスクランブルをかける方法。
【請求項１３】
前記マーキングキー（３６）にスペクトル拡散が行われることを特徴とする請求項１から１２のいずれか一項に記載のスクランブルをかける方法。
【請求項１４】
先行する画像のマーキングキーの置換によって得られるマーキングキー（３６）によって、各画像にスクランブルをかけることを特徴とする請求項１から１３のいずれか一項に記載のスクランブルをかける方法。
【請求項１５】
暗号解読キー（K_T）使用して、ビデオ信号（Ｓ）のスクランブルを解除する方法であって、前記スクランブル解除が、請求項１から１４のいずれか一項に記載の方法によってスクランブルをかけられた信号に行われることを特徴とするスクランブル解除方法。
【請求項１６】
前記スクランブル解除が、
前記ビデオ信号を符号化することによって得られる動きベクトルのセットから動きベクトル（V_6，V_5，V_2，V_9）を選択するステップと、
前記選択されたベクトルの横軸成分および縦軸成分を、それぞれ横軸ベクトル（V_x）および縦軸ベクトル（V_y）と呼ぶ２つのベクトルに分離するステップと、
一次元ＤＣＴ型変換を前記２つのベクトルの各々に適用するステップと、
前記暗号解除キーから導出されるマーキングキー（３６）を使用して、タトゥーイング関数を前記横軸ベクトルおよび前記縦軸ベクトルのＤＣＴ変換の成分（F_x，F_y）に適用するステップと、
前記横軸ベクトルおよび前記縦軸ベクトルに逆ＤＣＴ変換を適用し、前記選択された動きベクトルの新しい値を作成するためにそれらのベクトルを再結合させるステップと、
を含むことを特徴とする請求項１５に記載のスクランブル解除方法。
【請求項１７】
先行する画像のマーキングキーの置換によって得られるマーキングキーによって、各画像がスクランブル解除されることを特徴とする請求項１５または１６に記載のスクランブル解除方法。
【請求項１８】
動きを解析するための手段を含む符号化器であって、請求項１から１４のいずれか一項に記載の方法を実施することによって、ビデオ信号（Ｓ）にスクランブルをかけるための手段をさらに含むことを特徴とする符号化器。
【請求項１９】
請求項１５から１７のいずれか一項に記載のスクランブル解除方法を実施することによって、ビデオ信号（Ｓ）をスクランブル解除するための手段を含むことを特徴とする復号化器。
【請求項２０】
ビデオ信号（Ｓ）を一斉送信するためのサーバであって、請求項１から１４のいずれか一項に記載の方法を実施することによって、前記ビデオ信号（Ｓ）にスクランブルをかける

ための手段を含むことを特徴とするサーバ。
【請求項２１】
情報伝送ネットワーク（１４）上に一斉送信されるビデオ信号（Ｓ）を受信するための前記ネットワークへの接続のためのアクセスターミナル（１６）であって、請求項１５から１７のいずれか一項に記載の方法を実施することによって、前記ビデオ信号（Ｓ）をスクランブル解除するための手段を含むことを特徴とするターミナル。
【請求項２２】
請求項１から１４のいずれか一項に記載の方法を使用して、スクランブルがかけられたビデオ信号（Ｓ）を保存するための手段を含むことを特徴とするコンピュータ読出し可能なデータ媒体（１２）。
【請求項２３】
視聴覚情報へのアクセスを制御するために暗号化キー（K_T）を使用して、ビデオ信号（Ｓ）にスクランブルをかけ、スクランブルを解除するシステムであって、ビデオ信号（Ｓ）を保存するための保存手段（１２）に関連するビデオ信号を一斉送信するための一斉送信サーバ（１０）を含み、前記ビデオ信号（Ｓ）を一斉送信するための情報伝送ネットワーク（１４）に接続され、請求項１から１４のいずれか一項に記載の方法を実施することによって、前記ビデオ信号（Ｓ）にスクランブルをかけるための手段を含むことを特徴とするシステム。
【請求項２４】
スクランブルをかけ、スクランブルを解除するシステムであって、前記情報伝送ネットワーク（１４）に接続されるアクセスターミナル（１６）をさらに含み、前記アクセスターミナル（１６）が、請求項１５から１７のいずれか一項に記載の方法を実施することによって、前記ビデオ信号（Ｓ）をスクランブル解除するための手段を含むことを特徴とする請求項２３に記載のシステム。
【発明の詳細な説明】
媒体
【技術分野】
【０００１】
本発明は、一斉送信サーバによって送信される視聴覚情報へのアクセスを制御するために、暗号化キーを使用してビデオ信号にスクランブルをかける方法に関する。
【０００２】
本発明は、ビデオ信号をスクランブル解除する方法、および、前記方法を実施するためのシステム、符号化器、復号化器、一斉送信サーバ、および、データ媒体も提供する。
【背景技術】
【０００３】
視聴覚情報へのアクセスを制御するために実施されるスクランブル方法は数多く存在する。例えば、１つの解決策は、デジタルビデオ一斉送信（ＤＶＢ）協議会のＤＶＢスクランブリング法によって提供される。
【０００４】
これらの方法は、ビデオ信号にスクランブルをかけるために暗号化キーを一般に利用する。スクランブル化は、一般に、スクランブルをかけていないストリームと暗号化キーとの間に排他ＯＲ（ＸＯＲ）操作を行うことに基づく。
【０００５】
例えば、番組を一斉送信することに関して、視聴覚情報へのアクセスを所望するユーザは、スクランブルがかけられた信号を、中でも暗号化キーと関連した暗号解読キーを搬送するＭＰＥＧ－２　伝送ストリーム（ＭＰＥＧ－２　ＴＳ）パケットを表す権利付与制御メッセージ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ（ＥＣＭ））型のメッセージとともに受信する。ビデオをスクランブル解除するために使用するのは暗号解読キーである。
【０００６】

残念ながら、このタイプのスクランブル化の方法は、結果として、スクランブルがかけられているが視聴できないビデオ信号をユーザに供給することになる。スクランブルがかけられたビデオ信号は、スクランブル解除の前にユーザが視聴覚コンテンツについて何らかのヒントを得ることを可能にしない。

【考案の開示】

【発明が解決しようとする課題】

【０００７】

本発明は、ビデオコンテンツにスクランブルをかけることを可能にする一方、それにもかかわらず、コンテンツがある程度は可視のままであることを確実にするビデオ信号のスクランブル解除法を提供することによって、この欠点を救済しようと試みる。

【０００８】

この目的のために、本発明は、暗号化キーから導出されるマーキングキーを使用して、ビデオ信号にタトゥーイング関数を適用することによってビデオ信号にスクランブルをかけ、前記タトゥーイング関数が、ビデオ信号におけるタトゥーイングの可視性の調整を可能にするタトゥーイングの振幅を調節するためのパラメータを含むことを特徴とする上記に詳述したタイプのスクランブルをかける方法を提供する。

【課題を解決するための手段】

【０００９】

本発明のスクランブをかける方法は、１つまたは複数の以下の特徴をさらに含むことができる。

－視聴覚情報が一斉送信サーバからアクセス可能であること。

－視聴覚情報が読出しのためにアクセス可能であるデータ媒体に保存されること。

－タトゥーイング関数が、ビデオ信号を符号化することによって得られる動きベクトルに適用されること。

－タトゥーイング関数が前記動きベクトルの周波数表示に適用されること。

－スクランブルをかけることが以下のステップを含むこと。

・ビデオ信号を符号化することによって得られる動きベクトルのセットから動きベクトルを選択するステップと、

・選択されたベクトルの横軸成分および縦軸成分を、それぞれ横軸ベクトルおよび縦軸ベクトルと呼ぶ２つのベクトルに分離するステップと、

・一次元離散余弦変換（ＤＣＴ）型変換を前記２つのベクトルの各々に適用するステップと、

・マーキングキーを使用して、タトゥーイング関数を横軸ベクトルおよび縦軸ベクトルのＤＣＴ変換の成分に適用するステップ、および、

・タトゥーイングの後に、選択された動きベクトルに対して新しい値を提供するために、横軸ベクトルおよび縦軸ベクトルに逆ＤＣＴ変換を行い、それらのベクトルを再結合させるステップ。

－動きベクトルが、符号化されたビデオストリームから直接抽出され、符号化された後にビデオ信号にスクランブルをかけられること。

－ビデオ信号を符号化する間に動きベクトルが選択され、ビデオ信号が符号化される間にビデオ信号にスクランブルがかけられること。

－スクランブルをかけることが、オーサの権利に関する情報を含むタトゥーイングキーを使用してタトゥーイング関数を適用することによって、ビデオ信号の不可視タトゥーイングに組み合されること。

－オーサの権利の情報がビデオの識別子を含み、オーサの識別子がビデオに対する権利を有すること。

－ビデオ信号にスクランブルをかけるために、マーキングキーの代わりに使用される新しいマーキングキーを生成するための一対一対応を提供する関数を使用して、前記タトゥーイングキーがマーキングキーに結合されること。

－ビデオ信号がＭＰＥＧ－２またはＭＰＥＧ－４に準拠して符号化されること。

－マーキングキーにスペクトル拡散が行われること。および、
－先行する画像のマーキングキーの置換によって得られるマーキングキーによって、各画像にスクランブルをかけること。
【００１０】
本発明は、暗号解読キーを使用してビデオ信号のスクランブルを解除する方法であって、スクランブル解除が上記に説明したスクランブルをかける方法によって、スクランブルをかけられた信号に行われることを特徴とするスクランブル解除方法も提供する。
【００１１】
スクランブル解除の方法は１つまたは複数の以下の特徴を含むことができる。
－本方法が以下のステップを含むこと。
・ビデオ信号を符号化することによって得られる動きベクトルのセットから動きベクトルを選択するステップ。
・選択されたベクトルの横軸成分および縦軸成分を、それぞれ横軸ベクトルおよび縦軸ベクトルと呼ぶ２つのベクトルに分離するステップ。
・一次元ＤＣＴ型変換を前記２つのベクトルの各々に適用するステップ。
・暗号解除キーから導出されるマーキングキーを使用して、タトゥーイング関数を横軸ベクトルおよび縦軸ベクトルのＤＣＴ変換の成分に適用するステップ。および、
・横軸ベクトルおよび縦軸ベクトルに逆ＤＣＴ変換を適用し、選択された動きベクトルの新しい値を作成するためにそれらのベクトルを再結合させるステップ。
－先行する画像のマーキングキーの置換によって得られるマーキングキーによって、各画像がスクランブル解除されること。
【００１２】
本発明は、動きを解析するための手段を含む符号化器であって、上記に説明したスクランブル方法を実施することによって、ビデオ信号にスクランブルをかけるための手段をさらに含むことを特徴とする符号化器も提供する。
【００１３】
本発明は、上記に説明したスクランブル解除方法を実施することによって、ビデオ信号をスクランブル解除するための手段を含むことを特徴とする復号化器も提供する。
【００１４】
本発明は、ビデオ信号を一斉送信するためのサーバであって、上記に説明したスクランブル方法を実施することによって、ビデオ信号にスクランブルをかけるための手段を含むことを特徴とするサーバも提供する。
【００１５】
本発明は、情報伝送ネットワークに一斉送信されるビデオ信号を受信するための前記ネットワークへの接続のためのアクセスターミナルであって、上記に説明したスクランブル解除の方法を実施することによって、ビデオ信号をスクランブル解除するための手段を含むことを特徴とするターミナルも提供する。
【００１６】
本発明は、上記に説明したスクランブル方法を使用して、スクランブルがかけられたビデオ信号を保存するための手段を含むことを特徴とするコンピュータ読出し可能なデータ媒体も提供する。
【００１７】
最後に、本発明は、視聴覚情報へのアクセスを制御するために暗号化キーを使用して、ビデオ信号にスクランブルをかけ、スクランブルを解除するシステムであって、ビデオ信号を保存するための保存手段に関連するビデオ信号を一斉送信するための一斉送信サーバを含み、ビデオ信号を一斉送信するための情報伝送ネットワークに接続され、上記に説明したスクランブルをかける方法を実施することによって、ビデオ信号にスクランブルをかけるための手段を含むことを特徴とするシステムも提供する。
【００１８】
本発明のスクランブルをかけ、スクランブルを解除するシステムは、情報伝送ネットワー

クに接続されるアクセスターミナルを含み、前記アクセスターミナルが、上記に説明したスクランブル解除の方法を実施することによって、ビデオ信号をスクランブル解除するための手段を含むという特徴も含むことができる。

【００１９】

本発明は、純粋に実施例として与え、添付の図面を参照して行う以下の説明からさらに良く理解される。

【発明を実施するための最良の形態】

【００２０】

図１に示すシステムは、システムに接続されたデータベース１２内に保存される視聴覚情報を一斉送信するためのサーバ１０を含む。

【００２１】

一斉送信サーバ１０は従来型のものであり、例えば、一斉送信される視聴覚情報にスクランブルをかける方法を実施するためのランダムアクセスメモリ（ＲＡＭ）および読出し専用メモリ（ＲＯＭ）に接続される中央演算処理装置（ＣＰＵ）を含む。

【００２２】

一斉送信サーバ１０は、インターネットなどの情報伝送ネットワーク１４にも接続される。したがって、スクランブルをかけられた視聴覚情報は、このネットワークを介して少なくとも１つの識別されたクライアントターミナル１６に送信することができる。

【００２３】

従来のプロトコルを使用する安全なデータ交換のための手段は、一斉送信サーバ１０に、および、クライアントターミナル１６にも組み込まれる。

【００２４】

そのような安全なデータ交換手段の組み込みは、図４を参照して以下に説明する機密データを交換する方法を実施するために必要である。

【００２５】

図２に示すスクランブルをかける方法は、一斉送信サーバ１０のソフトウエアおよびハードウエア手段を使用して一斉送信サーバ１０によって実施される。一斉送信サーバ１０の機能は、スクランブルをかけるためにビデオ信号を処理することである。

【００２６】

この実施において、一斉送信サーバ１０は、入力としてソースビデオ信号（Ｓ）を受信し、出力としてネットワーク１４を介して一斉送信される前に変調される準備が整っている符号化された二進信号を送出するように構成される、例えば、ＭＰＥＧ－２符号化器などの符号化器２０を含む。

【００２７】

この場合、クライアントターミナル１６には、ソース信号Ｓを復号化して表示することを可能にするために、ＭＰＥＧ－２型の復号化器が設けられる。

【００２８】

一斉送信サーバ１０は、ＭＰＥＧ－４規格の符号化器も使用することができ、その場合、クライアントターミナル復号化器１６も、同様にＭＰＥＧ－４規格に準拠しなければならない。時間成分を含む多次元シーケンスにおける動きを走査する他のいかなる符号化器を使用することも可能である。

【００２９】

従来の方法では、符号化器２０は、動きベクトル２４のマトリクスをビデオ信号Ｓの所与の画像に関連付ける、動きを評価するためのモジュール２２を有する。

【００３０】

動きベクトルのこのマトリクスは、例えば動きベクトルに応じてビデオ信号の先行する画像の画素のマクロブロックを動かすことによってビデオ信号の先行する画像に基づいて、問題の画像の予測される画像を生成するために機能する。

【００３１】

結果として、復号化器が、考慮する画像を復元することを可能にするために、動きベクト

ルのマトリクス２４、および、考慮する画像とその予測される画像との間の差を取った結果である残存画像の内容のみを送信することが可能になる。先行する画像から開始すると、動きベクトルのマトリクス２４を使用して復号化する際に、予測される画像を再構成することが可能になり、したがって、送信された残存画像を予測される画像に加算することによって考慮する画像を復元することが可能になる。この従来の方法は、ビデオ信号Ｓを効率的に圧縮することを可能にする。

【００３２】

この図に示す動きベクトルのマトリクス２４は９個の動きベクトルV_1～V_9を含む。当然、動きベクトルの数は一般にこれより多い。以下の説明を明確にするために９個のみを示す。

【００３３】

ステップ２６で、一斉送信サーバ１０は、ビデオ信号Ｓに関連した暗号化キーK_Tを生成する。このキーは、対応する視聴覚データとともにデータベース１２に保存される。

【００３４】

その後、ステップ２８で、一斉送信サーバ１０は、前記暗号化キーから疑似無作為的な方法で、マトリクス２４の動きベクトルから動きベクトルのセット３０を選択する。この例において、動きベクトルの選択されたセットはベクトルV_6、V_5、V_2、V_9によって構成される。

【００３５】

その後、サーバ１０は、選択されたベクトルの横軸成分および縦軸成分を、それぞれ横軸ベクトルV_xおよび縦軸ベクトルV_yと呼ぶ２つのベクトルに分離する。したがって、ベクトルV_xは、以下のように、セット３０における４個のベクトルの横軸を表す４個の成分を含む。

$V_x = (V_{6x}, V_{5x}, V_{2x}, V_{9x})$

【００３６】

同様に、V_yは、以下のように、セット３０の４個のベクトルの縦軸から取られた４個の成分を含む。

$V_y = (V_{6y}, V_{5y}, V_{2y}, V_{9y})$

【００３７】

以下のステップ３２で、一斉送信サーバ１０は，一次元ＤＣＴ型の変換をこれらの２個のベクトルの各々に適用する。

【００３８】

これは、ベクトルV_xおよびV_yをそれぞれ表す２個のベクトルF_xおよびF_yを作成するが、周波数領域におけるものである。

【００３９】

これらの２個の新しいベクトルは以下の成分を有する。

$F_x = (F_{6x}, F_{5x}, F_{2x}, F_{9x})$、および、$F_y = (F_{6y}, F_{5y}, F_{2y}, F_{9y})$

【００４０】

暗号化キーを生成するステップ２６に続くステップ３４で、一斉送信サーバ１０は、ゼロの値が値－１によって置き換えられる暗号化キーK_Tの二進法版を表すマーキングキー３６を生成する。

【００４１】

スクランブルをさらに強固にするために、マーキングキー３６のスペクトルを拡散することが有利である。これを行うために、マーキングキーはオーバーサンプルされ、続いて、ランダムノイズがこれに加えられる。したがって、マーキングキーに冗長性が作られ、さらに、マーキングキーは、このノイズによってスクランブルがかけられる。

【００４２】

マーキングキーは、ステップ２８で選択された動きベクトルが存在する数と同じ数の二進成分を有する。すなわち、マーキングキー３６はベクトルF_xおよびF_yの各々と同じ数

の成分を有する。この例では、４個の二進成分を有するマーキングキー３６が示され、最初および最後の成分は値－１を有し、第２および第３の成分は値１を有する。

【００４３】

ステップ３４で得られるマーキングキー３６は、ステップ３８で、以下のタトゥーイング関数を適用することによって、選択された動きベクトルに挿入される。

もしW_i＝－１であれば、$F'X_i = FX_i + W_i \alpha$、および、$F'Y_i = FY_i$、

さもなければ、$F'X_i = FX_i$、および、$F'Y_i = FY_i + W_i \alpha$、

ここで、W_i、FX_i、FY_i、$F'X_i$、および、$F'Y_i$は、マーキングキー３６の、ベクトルF_xおよびF_yの、および、タトゥーイングの後のベクトルF_xおよびF_yに対する新しい値F_xおよびF_yのそれぞれｉ番目の成分を表す。

【００４４】

αはあらかじめ選択される係数であり、マーキングの強さを表す。αの値が大きくなるにつれ、選択された動きベクトルの周波数成分に対する修正も大きくなり、ビデオ信号においてスクランブルが可視となる程度も高くなる。

【００４５】

この操作の結果、ステップ３８を終了する際に、以下の２個のベクトルが得られる。

$F_x = (F_{6x}, F_{5x}, F_{2x}, F_{9x})$、および、$F_y = (F_{6y}, F_{5y}, F_{2y}, F_{9y})$

【００４６】

続いて、本方法はステップ４０に移り、ここで、全ての成分がベクトルV_xおよびV_yの成分とは異なる２つのベクトルV_xおよびV_yを出力するために、一斉送信サーバ１０が、ベクトルF_xおよびF_yに逆ＤＣＴ変換を適用する。したがって、選択された動きベクトルへのマーキングキー３６の挿入が、動きベクトルの全ての成分にわたって拡散していることが分かる。

【００４７】

その後、サーバ１０は、最初に選択されたベクトルV_6、V_5、V_2、V_9に対するスクランブルをかけられた値に対応する４個の動きベクトルのセット４２を再構成するために、ベクトルV_xおよびV_yの新しい成分を結合する。

【００４８】

これらの新しい動きベクトルはV_6、V_5、V_2、および、V_9と書かれる。

【００４９】

これらの新しいベクトルV_6、V_5、V_2、および、V_9は、動きベクトルの新しいマトリクス４４を提供するために、ベクトルV_6、V_5、V_2、および、V_9を置き換える。この新しいマトリクス４４は、復号化に際して、考慮する最初の画像のスクランブル版を得ることを可能にする。

【００５０】

マトリクス４４を動きベクトルのマトリクス２４から生成することを可能にするステップのセット、すなわち、ステップ２６、２８、３２、３４、３８、および、４０によって構成されるセットは、以下、スクランブラモジュールと呼ばれ、全体を通じた参照番号４６が与えられる。

【００５１】

符号化器２０において、従来の方法では、動きベクトルの全てのマトリクスにスクランブルをかけ、かつ、ネットワーク１４を介して一斉送信する前にデータベース１２に保存することができる、スクランブルがかけられた二進信号ＢＳ'を符号化器２０からの出力において得るために、ビデオ信号Ｓの各画像について動きの評価が繰り返される。

【００５２】

各繰り返しにおいて、マーキングキーをさらに検出困難にするために、後続のビデオ画像にマーキングキーを挿入する前に、マーキングキーに従来の置換を実施することが可能である。

【００５３】

あるいは、上述の方法は、ビデオ信号Ｓの不可視タトゥーイングの（図示しない）ステップを含む。

【００５４】

このタトゥーイングは従来の方法で行われ、例えば、上記に説明したものと同様であるが、タトゥーイングが不可視であるために十分低いαの値を備える関数などのタトゥーイング関数を信号に適用し、かつ第２のマーキングキーを使用する。この第２のマーキングキーは「タトゥーイングキー」と呼び、例えばビデオに権利を有するオーサの識別子によって構成される。

【００５５】

タトゥーイングのステップは、スクランブルとは独立に、かつ、スクランブラモジュール４６の前または後のいずれかで行うことができる。

【００５６】

タトゥーイングのステップはスクランブルをかけることと結合することもできる。「タトゥーされたマーキングキー」と呼ぶ新しいマーキングキーを生成するために、ＸＯＲ関数などの一対一対応を提供する関数を使用して、タトゥーイングキーとマーキングキー３６を相関させることが可能である。したがって、このタトゥーされたマーキングキーは、マーキングキー３６の代わりにスクランブラモジュール４６によって使用される。

【００５７】

相関関数の一対一の関係は、信号のタトゥーイングを必ずしも除去せずに、信号をスクランブル解除することができることを確実にすることを可能にする。

【００５８】

図３は、図２に示すスクランブルをかける方法の第２の実施を示す。

【００５９】

上記の実施例では、スクランブラモジュール４６を符号化器２０の一体化された部分であるとして、および、動き評価のステップ２２の後に動作するとして示すのに対し、図３の実施は、符号化器２０とは独立したスクランブラモジュール４６を示す。

【００６０】

この実施において、ビデオ信号Ｓは、符号化器２０の出力において二進信号ＢＳを供給するために符号化器２０によって最初に処理される。

【００６１】

続いて、二進信号ＢＳは、動きベクトルのマトリクス２４を自動的に抽出することが可能であるシンタックス分析器５８に入力される。以前と同様に、スクランブルがかけられた新しいマトリクス４４をスクランブラモジュール４６の出力において得るために、このマトリクス２４はスクランブラモジュール４６に入力される。

【００６２】

最後に、最後のステップ６０で、新しいマトリクス４４は、スクランブルがかけられた二進信号ＢＳ'を供給するために、二進信号ＢＳに再導入され、古いマトリクス２４を置き換える。この操作は、二進信号ＢＳにおける動きベクトルのマトリクスの全てについて行われる。

【００６３】

この実施において、上述のタトゥーイングのステップは、スクランブラモジュール４６とは独立に、または、スクランブルをかけることと組み合わせてのいずれでも同様に行うことができる。

【００６４】

クライアントターミナル１６には、ＭＥＰＧ－２規格と互換性を持つ復号化器が設けられているため、一斉送信サーバ１０によって一斉送信される二進信号ＢＳ'を復号化することが可能である。

【００６５】

加えて、もしクライアントターミナル１６が暗号化キーK_Tを所有していれば、これは、上述したように、スクランブラモジュール４６の双対である方法を実施することによって

、スクランブルをかけられた動きベクトルの本来の値を再構成することも可能である。スクランブル解除の方法と呼ぶ、この双対の方法を図５を参照して以下に詳細に説明する。

【００６６】

クライアントターミナル１６がスクランブル解除を行うことを可能にするために、暗号化キーK_Tを送信する方法を図４を参照して説明する。

【００６７】

第１のステップ５０で、クライアントターミナル１６は、一斉送信サーバ１０からスクランブルがかけられた二進ビデオ信号ＢＳ'をダウンロードする。

【００６８】

続くステップ５２で、ユーザターミナル１６は、一斉送信サーバ１０に、関心のあるビデオの内容を見るためにスクランブル解除のアプリケーションをダウンロードするように要求する。

【００６９】

この要求を受信すると、一斉送信サーバ１０は、識別子ＵＩＤ、および、識別子ＵＩＤおよびマスターキーK_Pにハッシング関数を適用することによって得られる秘密キーK_Sを生成する。

【００７０】

続くステップ５４で、一斉送信サーバはクライアントターミナル１６によって要求されたスクランブル解除のアプリケーションを送出する。安全な方法では、このアプリケーションは識別子ＵＩＤおよび秘密キーK_Sを含む。キーK_Sは、安全な方法でユーザターミナルによって保存される。したがって、ユーザはこれにアクセスできない。

【００７１】

したがって、ステップ５６で、ビデオを見るための権利を購入する方法が、クライアントターミナル１６と一斉送信サーバ１０との間で実施される。購入が行われれば、一斉送信サーバ１０は、ビデオコンテンツをスクランブル解除することを可能にする暗号化キーK_Tをデータベース１２から抽出し、一斉送信サーバ１０は、秘密キーK_Sに依存する暗号化関数E_{XS}を使用して暗号化キーK_Tを暗号化する。

【００７２】

これは暗号化された暗号化キーK_{SC}を作成する。

【００７３】

最後に、最後のステップ５８で、一斉送信サーバ１０は暗号化された暗号化キーをクライアントターミナル１６に送信する。

【００７４】

クライアントターミナルは、暗号化関数E_{KS}の双対である暗号解読関数D_{KS}を使用して、ダウンロードされたアプリケーションに保存された暗号化された暗号化キーおよび秘密キーK_Sから暗号化キーK_Tを復元することができる。

【００７５】

クライアントターミナル１６は図５に示す復号化器６０を含む。

【００７６】

復号化器６０は、入力として、スクランブルがかけられた二進ビデオ信号ＢＳ'を受信し、クライアントターミナル１６の表示画面に表示のために準備が整った、スクランブル解除され、復号化された信号Ｓを出力する。

【００７７】

復号化器６０は、動きベクトルを抽出するために特にモジュール６２を含む。この抽出モジュール６２は、マトリクス４４と同一の動きベクトルのマトリクス６４を出力する。

【００７８】

このマトリクス６４の少なくとも一部は、復号化器６０のスクランブル解除モジュール６６の入力に送出する、スクランブルがかけられた動きベクトルを含む。スクランブル解除モジュール６６は、動きベクトルの疑似無作為選択のための第１のステップ６８を含む方法を実施するための従来のソフトウエア手段を有する。このステップで、選択は、ステッ

プ２８におけるのと同じ方法で暗号化キーK_Tを使用して、すなわち、同じ疑似無作為選択アルゴリズムを使用して実施される。結果として、このステップで選択されるベクトルは、ステップ２８で選択されたベクトルと同じベクトルである。これはベクトルV_6、V_5、V_2、および、V_9のセット４２を構成する。

【００７９】

その後、これらの４個のベクトルの横軸成分および縦軸成分は、それぞれ横軸ベクトルV_xおよび縦軸ベクトルV_yと呼ぶ２つのベクトルに分離される。

【００８０】

続くステップ７０で、一次元ＤＣＴ型変換が、これらの２つのベクトルV_xおよびV_yの各々に適用される。

【００８１】

これは、周波数領域におけるベクトルV_xおよびV_yの各々を表す２つの上述のベクトルF_xおよびF_yを作成する。

【００８２】

ステップ３４と同一のステップ７２で、クライアントターミナル１６は、暗号化キーK_Tからマーキングキー３６を生成する。上記と同様の方法で、スペクトル拡散を、マーキングキー３６にも行うことができる。

【００８３】

ステップ７０に続くステップ７２で、ビデオ信号Ｓにスクランブルをかける間に選択された動きベクトルの成分に挿入されたマーキングキー３６が、上述のタトゥーイング関数の双対である以下の関数を適用することによって、次に、前記ベクトルから除去される。

もし$W_i = -1$であれば、$F'X_i = FX_i - W_i \alpha$、および、$F'Y_i = FY_i$、

さもなければ、$F'X_i = FX_i$、および、$F'Y_i = FY_i - W_i \alpha$、

【００８４】

この操作の結果として、ステップ７２を終了する際に、以下の２つのベクトルが得られる。

$F_x = (F_{6x}, F_{5x}, F_{2x}, F_{9x})$、および、$F_y = (F_{6y}, F_{5y}, F_{2y}, F_{9y})$

【００８５】

本方法は、続いて、ステップ７４に移り、ここで、スクランブル解除され、選択された動きベクトルの横軸成分および縦軸成分をそれぞれ含む２つのベクトルV_xおよびV_yを得るために、ベクトルF_xおよびF_yに逆ＤＣＴ変換が適用される。

【００８６】

その後、ベクトルV_xおよびV_yの成分は結合され、動きベクトルV_6、V_5、V_2、および、V_9を含むセット３０を再構成する。

【００８７】

結果として、スクランブル解除モジュール６６からの出力において、スクランブル解除された動きベクトルのマトリクス２４が供給される。

【００８８】

符号化の間に信号Ｓにスクランブルをかけることに関して、スクランブル解除は、図３を参照して説明した方法の双対である方法によって、復号化とは独立に行うことができる。

【００８９】

ビデオ信号にスクランブルをかけるための本発明の方法は、送信されるビデオ信号にスクランブルをかることを可能にするが、潜在的に関心を持つユーザがそのコンテンツを見ることを妨害することのないようにすることによって、有料視聴覚コンテンツの一斉送信を改善することが明らかに分かる。

【００９０】

上述の発明の他の長所は、これが、ビデオコンテンツの不可視タトゥーイングが、ビデオコンテンツにスクランブルをかけることと組み合わされることを可能にすることである。

【図面の簡単な説明】

【００９１】
【図１】本発明の方法を使用してビデオ信号を一斉送信するためのシステム構成を示す模式図である。
【図２】本発明のスクランブルをかける方法の第１の実施の様々なステップを示す図である。
【図３】本発明のスクランブルをかける方法の第２の実施の様々なステップを示す図である。
【図４】本発明の方法を使用してスクランブルがかけられたビデオ信号をスクランブル解除するためのキーを交換する方法を示す図である。
【図５】本発明のスクランブル解除の方法の様々なステップを示す図である。
【符号の説明】
【００９２】
１０　一斉送信サーバ
１２　データベース
１４　情報伝送ネットワーク
１６　クライアントターミナル
２０　符号化器
２４、４４、６４　マトリクス
３６　マーキングキー
４２　４つの動きベクトルのセット
４６　スクランブラモジュール
６０　復号化器
６２　抽出モジュール
６６　スクランブル解除モジュール

【図１】

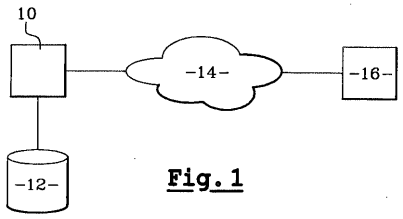

Fig. 1

【図２】

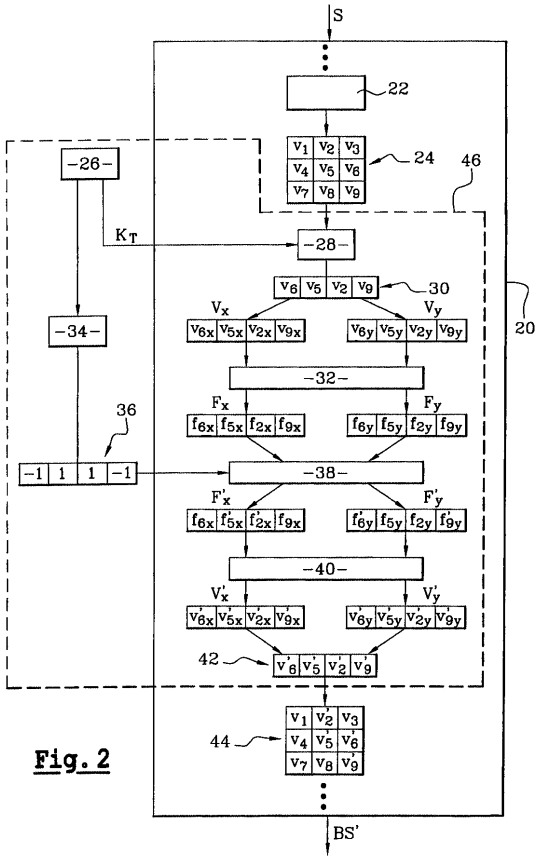

Fig. 2

【図３】

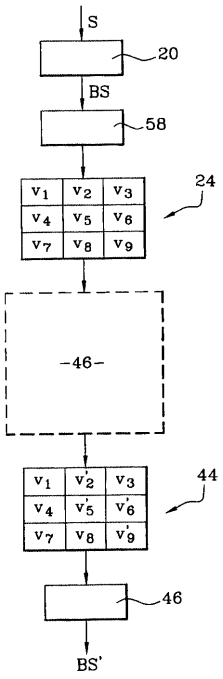

Fig. 3

【図４】

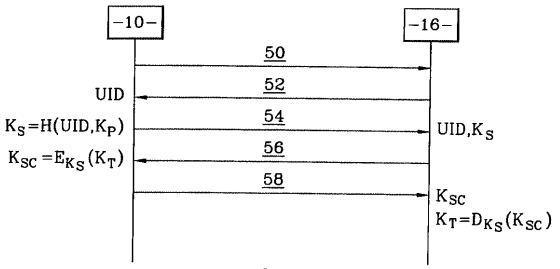

Fig. 4

【図５】

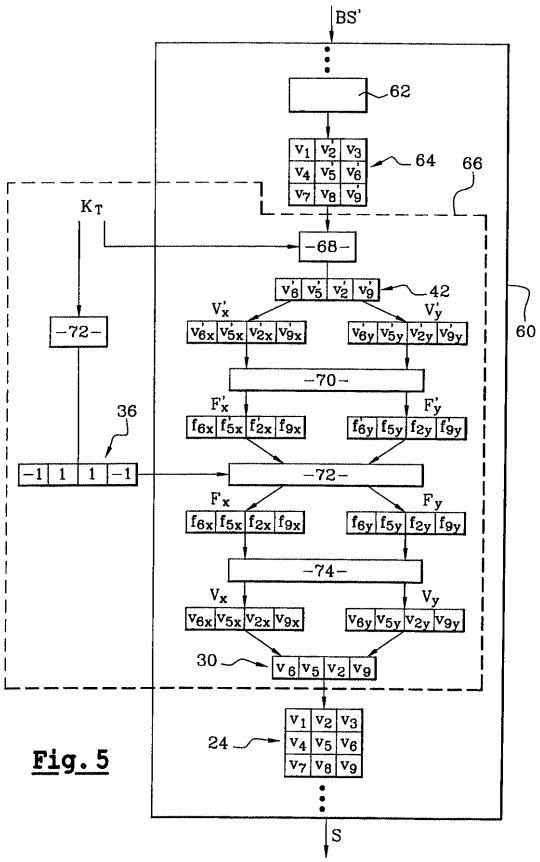

Fig. 5

フロントページの続き

(72)発明者　ヤン・ボド
フランス国、３５７００・レンヌ、スクワール・ドウ・サンデ・３
(72)発明者　ナタリー・ロラン
フランス国、３５６３０・ビニヨツク、リユ・デ・フレシユ・３
(72)発明者　クリストフ・ロラン
フランス国、３５６３０・ビニヨツク、リユ・デ・フレシユ・３

Ｆターム(参考)　5C064 BA01 BB02 BC06 BC17 BC22 BD08 BD09 CA14 CC04
5J104 AA01 AA39 BA03 EA04 EA18 JA03 NA02 NA15 PA05

【外国語明細書】

1. Title of Invention

METHODS OF SCRAMBLING AND UNSCRAMBLING A VIDEO SIGNAL, A SYSTEM, AN ENCODER, A DECODER, A BROADCAST SERVER, AND A DATA MEDIUM FOR IMPLEMENTING THE METHODS

2. Claims

1/ A method of scrambling a video signal (S) using an encryption key (K_T) for controlling access to audiovisual information, the method being characterized in that the video signal is scrambled by applying (38) a tattooing function to the video signal using a marking key (36) derived from the encryption key, the tattooing function including a parameter for regulating the amplitude of the tattooing that enables the visibility thereof in the video signal to be adjusted.

2/ A scrambling method according to claim 1, characterized in that the audiovisual information is accessible from a broadcast server (10).

3/ A scrambling method according to claim 1 or claim 2, characterized in that the audiovisual information is stored on a data medium (12) that is accessible for reading.

4/ A scrambling method according to any one of claims 1 to 3, characterized in that the tattooing function is applied to motion vectors (V_6, V_5, V_2, V_9) obtained by encoding (20) the video signal (S).

5/ A scrambling method according to claim 4, characterized in that the tattooing function is applied to a frequency representation (F_x, F_y) of said motion vectors.

6/ A scrambling method according to claim 5, characterized in that the scrambling comprises the following steps:

- selecting (28) motion vectors (V_6, V_5, V_2, V_9) from a set (24) of motion vectors obtained by encoding the video signal;

- separating abscissa and ordinate components of the selected vectors in two vectors respectively referred to as the abscissa vector (V_x) and the ordinate vector (V_y);

- applying (32) a one-dimensional DCT type transform to each of said two vectors;

- applying (38) the tattooing function using the marking key (36) to the components (F_x, F_y) of the DCT transforms of the abscissa and ordinate vectors; and

- performing an inverse DCT transform on the abscissa and ordinate vectors and recombining them so as to provide new values for the selected motion vectors, after tattooing.

7/ A scrambling method according to any one of claims 4 to 6, characterized in that the motion vectors (V_6, V_5, V_2, V_9) are extracted directly from the encoded video stream (BS), the video signal being scrambled (46) after being encoded (20).

8/ A scrambling method according to any one of claims 4 to 6, characterized in that the motion vectors (V_6, V_5, V_2, V_9) are selected while encoding (20) the video signal, the video signal then being scrambled (46) while it is being encoded.

9/ A scrambling method according to any one of claims 1 to 8, characterized in that the scrambling is combined with invisible tattooing of the video signal (S) by applying a tattooing function using a tattooing key including information concerning author rights.

10/ A scrambling method according to claim 9, characterized in that the author rights information includes an identifier (UID) of the video and an identifier of the author having rights over the video.

11/ A scrambling method according to claim 9 or claim 10, characterized in that said tattooing key is combined with the marking key (36) using a function presenting one-to-one correspondence to generate a new marking key used instead of the marking key (36) for scrambling the video signal (S).

12/ A scrambling method according to any one of claims 1 to 11, characterized in that the video signal (S) is encoded (20) in conformity with the MPEG-2 or the MPEG-4 standard.

13/ A scrambling method according to any one of claims 1 to 12, characterized in that spectrum spreading is performed on the marking key (36).

14/ A scrambling method according to any one of claims 1 to 13, characterized in that each image is scrambled by a marking key (36) obtained by permutation of the marking key of the preceding image.

15/ A method of unscrambling a video signal (S) using a decryption key (K_T), the method being characterized in that the unscrambling is performed on a signal scrambled by a method according to any one of claims 1 to 14.

16/ An unscrambling method according to claim 15, characterized in that the unscrambling comprises the following steps:

- selecting motion vectors (V'_6, V'_5, V'_2, V'_9) from a set of motion vectors obtained by encoding the video signal;
- separating the abscissa and ordinate components of the selected vectors in two vectors referred to respectively to as the abscissa vector (V'_x) and the ordinate vector (V'_y);

- applying a one-dimensional DCT type transform to each of said two vectors;

- applying a tattooing function using a marking key (36) derived from the decryption key to the components (F_x, F_y) of the DCT transforms of the abscissa and ordinate vectors; and

- applying an inverse DCT transform to the abscissa and ordinate vectors and recombining them to produce the new values of the selected motion vectors.

17/ An unscrambling method according to claim 15 or claim 16, characterized in that each image is unscrambled by a marking key obtained by permutation of the marking key of the preceding image.

18/ An encoder including means for analyzing motion, the encoder being characterized in that it further comprises means for scrambling a video signal (S) by implementing a method according to any one of claims 1 to 14.

19/ A decoder, characterized in that it includes means for unscrambling a video signal (S) by implementing an unscrambling method according to any one of claims 15 to 17.

20/ A server (10) for broadcasting a video signal (S), the server being characterized in that it includes means for scrambling the video signal (S) by implementing a method according to any one of claims 1 to 14.

21/ An access terminal (16) for connection to an information transmission network (14) to receive a video signal (S) broadcast over said network, the terminal being characterized in that it includes means for unscrambling the video signal (S) by implementing a method according to any one of claims 15 to 17.

22/ A computer-readable data medium (12), characterized in that it includes means for storing a video signal (S) that has been scrambled using a method according to any one of claims 1 to 14.

23/ A system for scrambling and unscrambling a video signal (S) using an encryption key (K_T) for controlling access to audiovisual information, the system comprising a broadcast server (10) for broadcasting the video signal (S) associated with storage means (12) for storing the video signal (S), and connected to an information transmission network (14) for broadcasting the video signal (S), the system being characterized in that it includes means for scrambling the video signal (S) by implementing a method according to any one of claims 1 to 14.

24/ A scrambling and unscrambling system according to claim 23, characterized in that it further comprises an access terminal (16) connected to the information transmission network (14), said access terminal (16) including means for unscrambling the video signal (S) by implementing a method according to any one of claims 15 to 17.

3. Detailed Description of Invention

The present invention relates to a method of scrambling a video signal using an encryption key for controlling access to audiovisual information transmitted by a broadcast server.

The invention also provides a method of unscrambling a video signal, and a system, an encoder, a decoder, a broadcast server, and a data medium for implementing said methods.

There exist numerous scrambling methods implemented for controlling access to audiovisual information. For example, one solution is provided by the DVB Scrambling method of the digital video broadcasting (DVB) consortium.

Those methods generally make use of an encryption key for scrambling the video signal. The scrambling is generally based on performing an exclusive-OR (XOR) operation between the non-scrambled stream and the encryption key.

For example, in the context of broadcasting programs, a user desiring to access audiovisual information receives the scrambled signal together with a message of the Entitlement Control Message (ECM) type which represents an MPEG-2 Transport Stream (MPEG-2 TS) packet conveying, amongst other things, a decryption key associated with the encryption key. It is the decryption key which is used for unscrambling the video.

Unfortunately, the result of that type of scrambling method is to supply the user with a video signal that is scrambled but that cannot be viewed. The scrambled video signal does not make it possible for the user to get some idea of the audiovisual content prior to unscrambling.

The present invention seeks to remedy that drawback by providing a method of unscrambling a video signal that enables the video content to be scrambled while

nevertheless ensuring that it remains viewable to some extent.

To this end, the invention provides a scrambling method of the above-specified type, characterized in that the video signal is scrambled by applying a tattooing function to the video signal using a marking key derived from the encryption key, the tattooing function including a parameter for regulating the amplitude of the tattooing that enables the visibility thereof in the video signal to be adjusted.

A scrambling method of the invention may further comprise one or more of the following characteristics:

- the audiovisual information is accessible from a broadcast server;
- the audiovisual information is stored on a data medium that is accessible for reading;
- the tattooing function is applied to motion vectors obtained by encoding the video signal;
- the tattooing function is applied to a frequency representation of said motion vectors;
- the scrambling comprises the following steps:
  . selecting motion vectors from a set of motion vectors obtained by encoding the video signal;
  . separating abscissa and ordinate components of the selected vectors in two vectors respectively referred to as the abscissa vector and the ordinate vector;
  . applying a one-dimensional Discrete Cosine Transform (DCT) type transform to each of said two vectors;
  . applying the tattooing function using the marking key to the components of the DCT transforms of the abscissa and ordinate vectors; and
  . performing an inverse DCT transform on the abscissa and ordinate vectors and recombining them so as to provide new values for the selected motion vectors, after tattooing;

- the motion vectors are extracted directly from the encoded video stream, the video signal being scrambled after being encoded;

- the motion vectors are selected while encoding the video signal, the video signal then being scrambled while it is being encoded;

- the scrambling is combined with invisible tattooing of the video signal by applying a tattooing function using a tattooing key including information concerning author rights;

- the author rights information includes an identifier of the video and an identifier of the author having rights over the video;

- said tattooing key is combined with the marking key using a function presenting one-to-one correspondence to generate a new marking key used instead of the marking key for scrambling the video signal;

- the video signal is encoded in conformity with the MPEG-2 or the MPEG-4 standard;

- spectrum spreading is performed on the marking key; and

- each image is scrambled by a marking key obtained by permutation of the marking key of the preceding image.

The invention also provides a method of unscrambling a video signal using a decryption key, the method being characterized in that the unscrambling is performed on a signal scrambled by a scrambling method as described above.

The unscrambling method may further comprise one or more of the following characteristics:

- it comprises the following steps:

  . selecting motion vectors from a set of motion vectors obtained by encoding the video signal;

  . separating the abscissa and ordinate components of the selected vectors in two vectors referred to respectively to as the abscissa vector and the ordinate vector;

. applying a one-dimensional DCT type transform to each of said two vectors;

. applying a tattooing function using a marking key derived from the decryption key to the components of the DCT transforms of the abscissa and ordinate vectors; and

. applying an inverse DCT transform to the abscissa and ordinate vectors and recombining them to produce the new values of the selected motion vectors; and

- each image is unscrambled by a marking key obtained by permutation of the marking key of the preceding image.

The invention also provides an encoder including means for analyzing motion, the encoder being characterized in that it further comprises means for scrambling a video signal by implementing a scrambling method as described above.

The invention also provides a decoder, characterized in that it includes means for unscrambling a video signal by implementing an unscrambling method as described above.

The invention also provides a video signal broadcast server characterized in that it includes means for scrambling the video signal by implementing a scrambling method as described above.

The invention also provides an access terminal for connection to an information transmission network to receive a video signal broadcast on the network, the terminal being characterized in that it includes means for unscrambling the video signal by implementing an unscrambling method as described above.

The invention also provides a computer-readable data medium, characterized in that it includes means for storing a video signal scrambled using a scrambling method as described above.

Finally, the invention also provides a system for scrambling and unscrambling a video signal using an encryption key for controlling access to audiovisual information, the system comprising a broadcast server for broadcasting the video signal associated with storage means for storing the video signal, and connected to an information transmission network for broadcasting the video signal, the system being characterized in that it includes means for scrambling the video signal by implementing a scrambling method as described above.

A scrambling and unscrambling system of the invention may also include the characteristic whereby it includes an access terminal connected to the information transmission network, said access terminal including means for unscrambling the video signal by implementing an unscrambling method as described above.

The invention will be better understood from the following description, given purely by way of example and made with reference to the accompanying drawings.

The system shown in Figure 1 comprises a server 10 for broadcasting audiovisual information stored in a database 12 connected thereto.

The broadcast server 10 is of conventional type and comprises, for example, a central processor unit (CPU)

associated with random access memory (RAM) and read-only memory (ROM) for implementing a method of scrambling audiovisual information that is to be broadcast.

The broadcast server 10 is also connected to an information transmission network 14, such as the Internet. Scrambled audiovisual information can thus be transmitted via this network to at least one identified client terminal 16.

Means for secure data exchange using a conventional protocol are installed on the broadcast server 10 and also on the client terminal 16.

The installation of such secure data exchange means is necessary for implementing a method of exchanging confidential data, as described below with reference to Figure 4.

The scrambling method shown in Figure 2 is implemented by the broadcast server 10 using its software and hardware means. Its function is to process a video signal in order to scramble it.

In this implementation, the broadcast server 10 includes an encoder 20, e.g. an MPEG-2 encoder, adapted to receive as input a source video signal S and to deliver as output an encoded binary signal ready to be modulated prior to being broadcast over the network 14.

In this case, the client terminal 16 is provided with an MPEG-2 type decoder in order to be able to decode and display the source signal S.

The broadcast server 10 can also use an MPEG-4 standard encoder, in which case the client terminal decoder 16 must likewise comply with the MPEG-4 standard. It is also possible to use any other encoder that scans motion in a multidimensional sequence including a time component.

In conventional manner, the encoder 20 has a module 22 for estimating motion which associates a matrix of motion vectors 24 with a given image of the video signal S.

This matrix of motion vectors serves to generate a predicted image of the image in question on the basis, for example, of the preceding image of the video signal, by moving macroblocks of pixels thereof as a function of the motion vectors.

As a result, it is possible to transmit only the matrix 24 of motion vectors and the content of a residual image that is the result of taking the difference between the image under consideration and its predicted image, in order to enable the decoder to restore the image under consideration. Starting from the preceding image, it is possible to reconstruct the predicted image on decoding using the matrix 24 of motion vectors, and it is then possible to restore the image under consideration by adding the transmitted residual image to the predicted image. This conventional method enables the video signal S to be compressed efficiently.

The matrix 24 of motion vectors shown in this figure comprises nine motion vectors V_1 to V_9. Naturally, the number of motion vectors is generally greater. Only nine are shown in order to clarify the description below.

During a step 26, the broadcast server 10 generates an encryption key K_T associated with the video signal S. This key is stored in the database 12 together with the corresponding audiovisual data.

Thereafter, during a step 28, the broadcast server 10 selects in pseudo-random manner from said encryption key a set 30 of motion vectors from the motion vectors of the matrix 24. In this example, the selected set of motion vectors is constituted by the vectors V_6, V_5, V_2, and V_9.

Thereafter, the server 10 separates the abscissa and ordinate components of the selected vectors into two vectors referred respectively as the abscissa vector V_x and the ordinate vector V_y. Thus, the vector V_x comprises four components representing the abscissas of the four vectors in the set 30, i.e.:

$$V_x = (V_{6x}, V_{5x}, V_{2x}, V_{9x})$$

Similarly, V_y comprises four components taken from the ordinates of the four vectors of the set 30, i.e.:

$$V_y = (V_{6y}, V_{5y}, V_{2y}, V_{9y})$$

During following step 32, the broadcast server 10 applies a transform of the one-dimensional DCT type to each of these two vectors.

This produces two vectors F_x and F_y representing the vectors V_x and V_y respectively, but in the frequency domain.

These two new vectors have the following components:

$F_x = (F_{6x}, F_{5x}, F_{2x}, F_{9x})$ and $F_y = (F_{6y}, F_{5y}, F_{2y}, F_{9y})$

During a step 34 following the step 26 of generating the encryption key, the broadcast server 10 generates a marking key 36 representing a binary version of the encryption key K_T, in which zero values are replaced by the value -1.

In order to make the scrambling even more robust, it is advantageous also to spread the spectrum of the marking key 36. To do this, the marking key is oversampled and then random noise is added thereto. Redundancy is thus created in the marking key which is, in addition, scrambled by the noise.

The marking key has as many binary components as there are motion vectors selected during step 28, i.e. the marking key 36 has as many components as each of the vectors F_x and F_y. In this example, a marking key 36 is shown that has four binary components, with the first and last components having the value -1 and the second and third components having the value 1.

The marking key 36 obtained during step 34 is inserted into the selected motion vectors during a step 38 by applying the following tattooing function:

if $W_i = -1$, then $F'X_i = FX_i + W_i\alpha$ and $F'Y_i = FY_i$,

else $F'X_i = FX_i$ and $F'Y_i = FY_i + W_i\alpha$,

where W_i, FX_i, FY_i, $F'X_i$, and $F'Y_i$ represent, respectively, the i-th components of the marking key 36,

of the vectors F_x and F_y, and of new values F'_x and F'_y for the vectors F_x and F_y after tattooing.

α is a coefficient that is selected a priori, representing the strength of the marking. The greater the value of α, the greater the modification to the frequency components of the selected motion vectors, and the greater the extent to which the scrambling is visible in the video signal.

As a result of this operation, on leaving step 38, the following two vectors are obtained:

$F'_x = (F_{6x}, F'_{5x}, F'_{2x}, F_{9x})$ and $F'_y = (F'_{6y}, F_{5y}, F_{2y}, F'_{9y})$

The method then moves onto a step 40 during which the broadcast server 10 applies an inverse DCT transform to the vectors F'_x and F'_y so as to output two vectors V'_x and V'_y in which all of the components differ from the components of the vectors V_x and V_y. Thus, it can be seen that the insertion of the marking key 36 into the selected motion vectors is spread over all of the components thereof.

Thereafter, the server 10 combines the new components of the vectors V'_x and V'_y so as to reconstitute a set 42 of four motion vectors corresponding to scrambled values for the initially selected vectors V_6, V_5, V_2, and V_9.

These new motion vectors are written V'_6, V'_5, V'_2, and V'_9.

These new vectors V'_6, V'_5, V'_2, and V'_9 replace the vectors V_6, V_5, V_2, and V_9 in order to provide a new matrix 44 of motion vectors. This new matrix 44 makes it possible on decoding to obtain a scrambled version of the initial image under consideration.

The set of steps enabling the matrix 44 to be generated from the matrix 24 of motion vectors, i.e. the set constituted by the steps 26, 28, 32, 34, 38, and 40 is referred to below as the scrambler module and is given an overall reference 46.

In the encoder 20, in conventional manner, motion estimation is reiterated on each image of the video signal S so as to obtain, at the output from the encoder 20, a scrambled binary signal BS' in which all of the matrices of motion vectors are scrambled, and which can be stored in the database 12 prior to being broadcast over the network 14.

On each iteration, it is possible to implement a conventional permutation on the marking key prior to inserting it in the following video image so as to make the key even more difficult to detect.

Optionally, the above-described method includes a step (not shown) of invisible tattooing of the video signal S.

This tattooing is performed in conventional manner by applying a tattooing function to the signal, for example a function similar to that described above, but with a value for α that is low enough for the tattooing to be invisible, and using a second marking key. This second marking key, referred to as the "tattooing key" is constituted, for example, by an identifier of the author having rights in the video.

The tattooing step can be performed independently of the scrambling, and either before or after the scrambler module 46.

The tattooing step may also be combined with scrambling. It is possible to correlate the tattooing key and the marking key 36 using a function providing one-to-one correspondence such as an XOR function so as to generate a new marking key referred to as the "tattooed marking key". This tattooed marking key is then used by the scrambler module 46 instead of the marking key 36.

The one-to-one relationship of the correlation function makes it possible to ensure that the signal can be unscrambled without necessarily removing its tattooing.

Figure 3 shows a second implementation of the scrambling method shown in Figure 2.

Whereas in the preceding example, the scrambler module 46 is shown as being an integral portion of the encoder 20 and as operating after a step 22 of estimating motion, the implementation of Figure 3 shows a scrambler module 46 that is independent of the encoder 20.

In this implementation, the video signal S is initially processed by the encoder 20 to provide a binary signal BS at its output.

The binary signal BS is then input to a syntax analyzer 58 capable of automatically extracting the matrix 24 of motion vectors. As before, this matrix 24 is input to the scrambler module 46 so as to obtain, at the output thereof, a new matrix 44 that is scrambled.

Finally, during a last step 60, the new matrix 44 is reintroduced into the binary signal BS, replacing the old matrix 24 so as to provide the scrambled binary signal BS'. This operation is performed on all of the matrices of motion vectors in the binary signal BS.

In this implementation, the above-described tattooing step can likewise be performed either independently of the scrambler module 46, or in combination with scrambling.

Since the client terminal 16 is provided with a decoder that is compatible with the MPEG-2 standard, it is capable of decoding the binary signal BS' broadcast by the broadcast server 10.

In addition, if the client terminal 16 possesses the encryption key K_T, it is also capable of reconstituting proper values for the scrambled motion vectors by implementing a method that is the dual of the scrambler module 46 as described above. This dual method, referred to as an unscrambler method, is described in detail below with reference to Figure 5.

To enable the client terminal 16 to perform unscrambling, a method of transmitting the encryption key K_T is described with reference to Figure 4.

During a first step 50, the client terminal 16 downloads a scrambled binary video signal BS' from the broadcast server 10.

During the following step 52, the user terminal 16 requests the broadcast server 10 to download an unscrambling application to view the content of the video of interest.

On receiving this request, the broadcast server 10 generates an identifier UID and a secret key K_S obtained by applying a hashing function to the identifier UID and a master key K_P.

During the following step 54, the broadcast server send the unscrambling application requested by the client terminal 16. In secure manner, this application includes the identifier UID and the secret key K_S. The key K_S is stored by the user terminal in a manner that is secure. Therefore the user cannot access it.

Thereafter, during a step 56, a method of purchasing the rights to view the video is implemented between the client terminal 16 and the broadcast server 10. Once purchase has been performed, the broadcast server 10 extracts from the database 12 the encryption key K_T that enables the video content to be unscrambled and it enciphers it using an encryption function E_{KS} which depends on the secret key K_S.

This produces an enciphered encryption key K_{SC}.

Finally, during a final step 58, the broadcast server 10 transmits the enciphered encryption key to the client terminal 16.

The client terminal can restore the encryption key K_T from the enciphered encryption key and the secret key K_S stored in the downloaded application, using a decryption function D_{KS} that is the dual of the encryption function E_{KS}.

The client terminal 16 includes a decoder 60 shown in Figure 5.

The decoder 60 receives as input the scrambled binary video signal BS' and it outputs the unscrambled and decoded signal S ready for display on a display screen of the client terminal 16.

The decoder 60 includes in particular a module 62 for extracting motion vectors. This extraction module 62 outputs a matrix 64 of motion vectors identical to the matrix 44.

At least part of this matrix 64 comprises motion vectors that are scrambled, which it delivers to the input of an unscrambler module 66 of the decoder 60. The unscrambler module 66 has conventional software means for implementing a method comprising a first step 68 for pseudo-random selection of motion vectors. During this step, the selection is implemented using the encryption key K_T in the same manner as the in step 28, i.e. using the same pseudo-random selection algorithm. As a result, the vectors that are selected during this step are the same vectors as those that were selected during the step 28. This constitutes the set 42 of vectors V'_6, V'_5, V'_2, and V'_9.

Thereafter, the abscissa and ordinate components of these four vectors are separated into two vectors referred to respectively as the abscissa vector V'_x and the ordinate vector V'_y.

During the following step 70, a one-dimensional DCT type transform is applied to each of these two vectors V'_x and V'_y.

This produces the two above-described vectors F'_x and F'_y, representing each of the vectors V'_x and V'_y in the frequency domain.

During a step 72 identical to the step 34, the client terminal 16 generates the marking key 36 from the encryption key K_T. In the same manner as above, spectrum spreading may also be performed on the marking key 36.

During the step 72 following the step 70, the marking key 36 which was inserted in the components of the motion vectors selected during scrambling of the video signal S, is now removed from said vectors by applying the following function, which is a dual of the above-described tattooing function:

if $W_i = -1$, then $F'X_i = FX_i - W_i\alpha$ and $F'Y_i = FY_i$,

else $F'X_i = FX_i$ and $F'Y_i = FY_i - W_i\alpha$,

As a result of this operation, on leaving step 72, the following two vectors are obtained:

$F_x = (F_{6x}, F_{5x}, F_{2x}, F_{9x})$ and $F_y = (F_{6y}, F_{5y}, F_{2y}, F_{9y})$

The method then moves onto a step 74 during which an inverse DCT transform is applied to the vectors F_x and F_y to obtain the two vectors V_x and V_y respectively comprising the abscissa components and the ordinate components of the unscrambled selected motion vectors.

Thereafter, the components of the vectors V_x and V_y are combined so as to reconstitute the set 30 comprising the motion vectors V_6, V_5, V_2, and V_9.

As a result, at the output from the unscrambler module 66, there is provided the matrix 24 of unscrambled motion vectors.

As for scrambling the signal S during encoding, unscrambling can be performed independently of decoding, by a method that is the dual of the method described with reference to Figure 3.

It can clearly be seen that a method of the invention for scrambling a video signal makes it possible to improve the broadcasting of paid-for audiovisual content by enabling the transmitted video signal to be scrambled but without preventing it being viewed by a user who is potentially interested.

Another advantage of the above-described invention is that it enables invisible tattooing of the video content to be combined with scrambling thereof.

4. Brief Description of Drawings

- Figure 1 is a diagram showing the structure of a system for broadcasting a video signal using a method of the invention.

- Figure 2 shows the various steps of a first implementation of the scrambling method of the invention.

- Figure 3 shows the various steps of a second implementation of a scrambling method of the invention.

- Figure 4 shows a method of exchanging keys for unscrambling a video signal scrambled using a method of the invention.

- Figure 5 shows the various steps of an unscrambling method of the invention.

1. Abstract

The invention relates in particular to a method of scrambling a video signal (S) using an encryption key (K_T) for controlling access to audiovisual information. The video signal is scrambled by applying (38) a tattooing function to the video signal by using a marking key (36) derived from the encryption key, the tattooing function including a parameter for regulating the amplitude of tattooing so as to enable the visibility of the tattooing in the video signal to be adjusted. The invention also provides a dual unscrambling method, and a system, an encoder, a decoder, a broadcast server, and a data medium for implementing said methods.

2. Representative Drawing

Fig. 2

Fig. 1

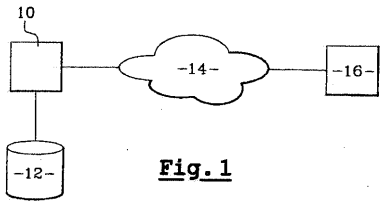

Fig. 1

Fig. 2

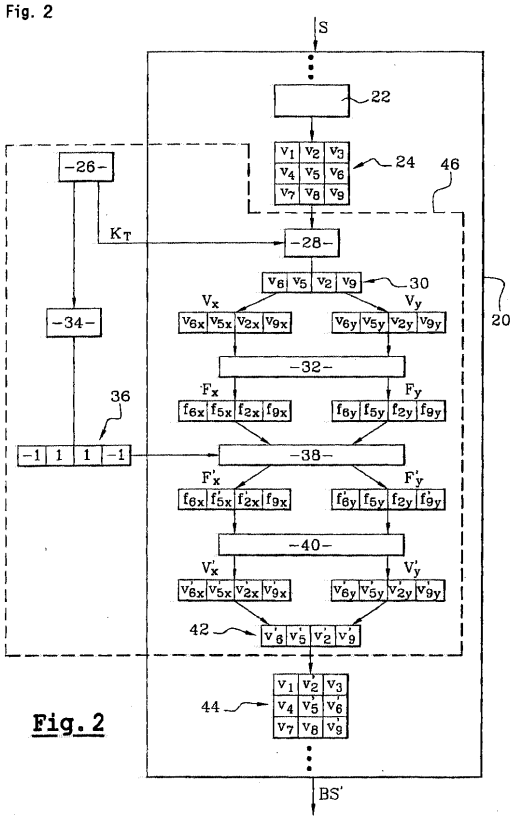

Fig. 2

Fig. 3

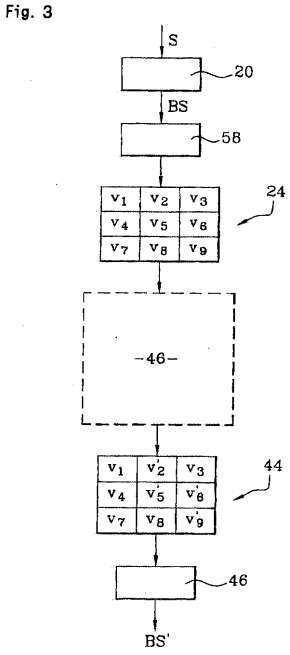

Fig. 3

Fig. 4

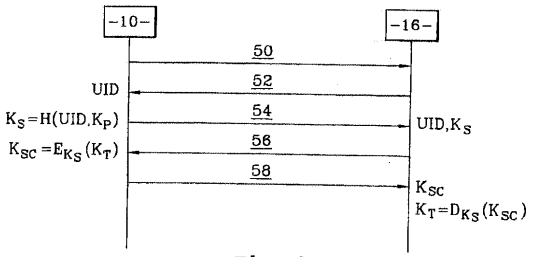

Fig. 4

Fig. 5

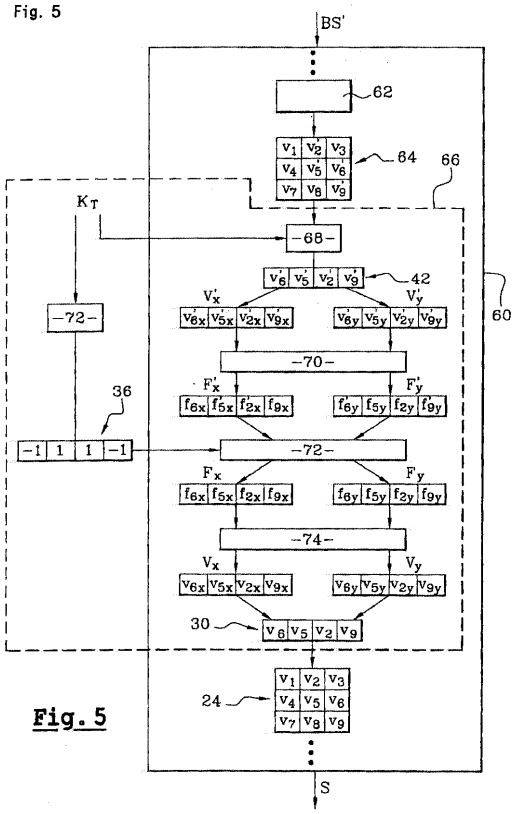
BS'
62
64
66
K_T
-68-
42
60
V'_x
V'_y
-72-
-70-
36
F'_x
F'_y
-1 1 1 -1
-72-
F_x
F_y
-74-
V_x
V_y
30
24
S

Fig. 5