

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4054590号
(P4054590)

(45) 発行日 平成20年2月27日(2008.2.27)

(24) 登録日 平成19年12月14日(2007.12.14)

(51) Int.Cl.

F I

H O 4 N 1/387 (2006.01)

H O 4 N 1/387

H O 4 N 1/00 (2006.01)

H O 4 N 1/00 1 O 7 Z

G O 6 T 1/00 (2006.01)

G O 6 T 1/00 5 O O B

H O 4 N 7/08 (2006.01)

H O 4 N 7/08 Z

H O 4 N 7/081 (2006.01)

請求項の数 4 (全 13 頁)

(21) 出願番号 特願2002-77838 (P2002-77838)
 (22) 出願日 平成14年3月20日(2002.3.20)
 (62) 分割の表示 特願平11-93000の分割
 原出願日 平成11年3月31日(1999.3.31)
 (65) 公開番号 特開2002-359737 (P2002-359737A)
 (43) 公開日 平成14年12月13日(2002.12.13)
 審査請求日 平成18年3月30日(2006.3.30)

(73) 特許権者 000001007
 キヤノン株式会社
 東京都大田区下丸子3丁目30番2号
 (74) 代理人 100090273
 弁理士 國分 孝悦
 (72) 発明者 岩村 恵市
 東京都大田区下丸子3丁目30番2号 キ
 ヤノン株式会社内

審査官 橋爪 正樹

(56) 参考文献 特開平11-041445 (JP, A)
 特開平11-075055 (JP, A)
 特開平10-271318 (JP, A)

最終頁に続く

(54) 【発明の名称】 情報監視システム

(57) 【特許請求の範囲】

【請求項1】

共通透かし埋込装置および複数の機関装置がネットワークを介して接続された情報監視システムであって、

前記共通透かし埋込装置が、

前記複数の機関装置の1つからのデジタルデータを登録する登録手段と、

前記デジタルデータと対応する機関装置において独自に用いられる電子透かし方式を示す独自透かし方式情報を、前記複数の機関装置に対して共通の電子透かし方式によって、前記デジタルデータに埋め込む共通透かし埋め込み手段と、

前記共通透かし埋め込み手段により前記独自透かし方式情報が埋め込まれたデジタルデータを前記デジタルデータと対応する機関装置に送信する送信手段とを備え、

前記機関装置が、

前記送信手段において送信されたデジタルデータに前記独自透かし方式情報とは異なる任意の情報を前記デジタルデータと対応する機関装置において独自に用いられる電子透かし方式によって埋め込む独自透かし埋め込み手段を備えたことを特徴とする情報監視システム。

【請求項2】

透かし抽出装置が更にネットワークを介して接続され、

前記透かし抽出装置が、

前記独自透かし埋め込み手段により任意の情報が埋め込まれたデジタルデータを取得す

10

20

る取得手段と、

前記取得手段により取得されたデジタルデータから前記独自透かし方式情報を前記共通の電子透かし方式と対応する抽出方式によって抽出する共通透かし抽出手段と、

前記共通透かし抽出手段において抽出された独自透かし方式情報に基づいて特定される抽出方式によって前記任意の情報を前記取得手段により取得されたデジタルデータから抽出する独自透かし抽出手段とを備えたことを特徴とする請求項 1 記載の情報監視システム

。

【請求項 3】

前記独自透かし抽出手段により前記任意の情報が抽出されなかった場合、前記任意の情報が破壊されたと判断することを特徴とする請求項 2 記載の情報監視システム。

10

【請求項 4】

前記任意の情報は、著作権情報、利用者情報及び識別情報のうちの少なくとも 1 つであることを特徴とする請求項 1 乃至 3 の何れか 1 項記載の情報監視システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル画像データやデジタル音声データ等の入力情報に付加情報を付加することにより著作権の保護、偽造防止、各種情報記録等を行う場合に用いて好適な情報監視システムに関するものである。

【0002】

20

【従来の技術】

近年のコンピュータ及びネットワークの発達は著しく、文字データ、画像データ、音声データ等、多種の情報がコンピュータ内、ネットワーク内で扱われるようになってきている。このようなデータはデジタルデータであるために、同質のデータの複製を容易に作成できる環境にある。このため、こうしたデータの著作権を保護するために、画像データや音声データの中に著作権情報や利用者情報を電子透かし情報（以下、単に電子透かしという）として埋め込む処理がなされる場合が多い。

【0003】

ここで、電子透かしとは、画像データや音声データに所定の処理を施すことによって、これらのデータの中に、人間の視覚や聴覚では認識できないような別の情報を密かに埋め込む技術である。この電子透かしを画像データや音声データから抽出することにより、著作権情報や利用者情報、及び識別情報などを得ることができ、不正コピーを追跡することが可能となる。

30

【0004】

このような電子透かしに求められる第 1 の条件は、埋め込まれた情報が知覚できない、即ち、元のデジタル情報の品質を劣化させることが少ないように埋め込めることである（品質）。

第 2 の条件は、デジタル情報の中に埋め込まれた情報が残り続ける、即ち、データ圧縮やフィルタ処理のような編集や攻撃を受けても、埋め込まれた情報が失われないことである（耐性）。

40

第 3 の条件は、用途に応じて埋め込める情報の情報量が選択できることである（情報量）。

【0005】

電子透かしに求められるこれらの条件は、一般的に互いにトレードオフの関係にある。例えば、耐性の強い電子透かしを実現しようとした場合、比較的大きな品質劣化が生じ、また埋め込む情報量が少なくなることが多い。

【0006】

また、多値の静止画像を例にとると、電子透かしを埋め込む方法として、空間領域に埋め込む方式と周波数領域に埋め込む方法との二つに大きく分類でき、下記のような種々の方法が知られている。

50

空間領域に埋め込む方式の例としては、パッチワークによるものとしてIBMの方式(W. Bender, D. Gruhl, N. Morimoto, Techniques for Data Hiding, "proceedings of the SPIE, San Jose CA, USA, February 1995)やG. B. Rhoads, W. Linn: "Steganography method employing embedded", USP Patent Number 5,636,292などが挙げられる。

【0007】

また、周波数領域に埋め込む方式の例としては、離散コサイン変換を利用するものとして、NTTの方式(中村、小川、高嶋、"デジタル画像の著作権保護のための周波数領域における電子透かし方式"、SCIS'97-26A, 1997年1月)の他に、離散フーリエ変換を利用するものとして、防衛大の方式(大西、岡、松井、"PN系列による画像への透かし署名法"、SCIS'97-26B, 1997年1月)や、離散ウェーブレット変換を利用するものとして、三菱、九大の方式(石塚、坂井、櫻井、"ウェーブレット変換を用いた電子透かし技術の安全性と信頼性に関する実験的考察"、SCIS'97-26D, 1997年1月)及び松下の方式("ウェーブレット変換に基づくデジタル・ウォーターマーク - 画像圧縮、変換処理に対するロバスト性について - ", 井上、宮崎、山本、桂、SCIS'98-3.2.A, 1998年1月)などが挙げられる。

【0008】

以上のような方式は、電子透かしの埋め込み処理と抽出処理とは一対一に対応しており、基本的に互換性はない。また、一般に空間領域に埋め込む手法は、品質劣化は少ないが耐性が弱く、周波数変換を用いる手法は、品質劣化は比較的大きいが耐性が強いと言われており、耐性は強いが埋め込める情報量が少ない手法や、品質は良いが耐性の弱い手法など方式毎にその特徴は異なる。

【0009】

さらに、これらの電子透かしは埋め込まれている情報を守るために、そのアルゴリズムや埋め込み位置や変化量などを示す情報(以後、鍵という)は秘密にされる場合が多い。これは、アルゴリズムや埋め込み位置等を解析することによって電子透かしを除去しようとする故意の攻撃に対する耐性を強くするためである。

【0010】

一方、効率的に著作権を保護するために、電子透かしの抽出等を行い不正コピーが行われていないかどうかを検査する監視機関を設けることが考えられる。このような監視機関において上記故意の攻撃を避けるために、電子透かし方式や鍵の守秘性を保持することは重要である。

【0011】

【発明が解決しようとする課題】

以上のように電子透かし方式にはその特徴に応じて種々の方式がある。また、電子透かしを用いてデジタルデータの不正コピー、及び不正出力を防止しようという企業、機関も多い。しかし、それらの企業、機関が独立に電子透かし方式を選択してデータに電子透かしを埋め込んだ場合、電子透かし方式の埋め込み処理と抽出処理は一対一に対応しており互換性がないために、以下のような問題が生じる。

【0012】

1 電子透かしの抽出処理を方式毎に行わなければならないので、1つの監視機関による統一的な検査が困難である。

2 1つの監視機関によって統一的に検査を行う場合、その監視機関は全ての電子透かし抽出手法を準備しておく必要があり負荷が大きい。

3 監視機関は、全ての抽出手法に対応する鍵を秘密かつ厳重に管理する必要がある。

4 方式毎に監視機関をもつとした場合、埋め込まれた透かしが抽出できなかったとき、他の方式による透かしが入っているのか、透かしが攻撃によって壊されたのか判定できない。

10

20

30

40

50

尚、ここで1つの監視機関とは、物理的に1つという意味ではなく、標準化や国等によって定められた組織的又は方式的に1つの体制を指す。

【0013】

本発明は上記の問題点に鑑みてなされたものであり、種々の電子透かし方式に対して効率的に著作物の保護等を実現することを目的としている。

【0014】

【課題を解決するための手段】

上記目的を達成するために、本発明の情報監視システムは、共通透かし埋込装置および複数の機関装置がネットワークを介して接続された情報監視システムであって、前記共通透かし埋込装置が、前記複数の機関装置の1つからのデジタルデータを登録する登録手段と、前記デジタルデータと対応する機関装置において独自に用いられる電子透かし方式を示す独自透かし方式情報を、前記複数の機関装置に対して共通の電子透かし方式によって、前記デジタルデータに埋め込む共通透かし埋め込み手段と、前記共通透かし埋め込み手段により前記独自透かし方式情報が埋め込まれたデジタルデータを前記デジタルデータと対応する機関装置に送信する送信手段とを備え、前記機関装置が、前記送信手段において送信されたデジタルデータに前記独自透かし方式情報とは異なる任意の情報を前記デジタルデータと対応する機関装置において独自に用いられる電子透かし方式によって埋め込む独自透かし埋め込み手段を備えたことを特徴とする。

10

【0020】

【発明の実施の形態】

20

(第1の実施の形態)

図1は、本発明の第1の実施の形態による情報処理システムにおける電子透かしの埋め込みに関する部分を示したものである。特に、各監視機関独自の電子透かし方式と共通の電子透かし方式とをもつシステムを示したものである。ここで、共通の電子透かし方式とは、標準化又は関係する機関間で定められた電子透かし方式であり、その特徴は後述する。

【0021】

図1において、101～104は異なる独自の電子透かし方式を用いて埋め込み処理を行う機関を示す。また、各機関101～104における各105は、定められた共通の電子透かし方式による埋め込み処理を行う共通透かし埋込装置であり、106～109は、各機関101～104毎に定めた独自の電子透かし方式による埋め込み処理を行うA～D透かし埋込装置である。110は各機関をつなぐネットワークであり、図示はしないが各機関101～104はこのネットワーク110に接続する通信手段を有している。

30

【0022】

共通透かし埋込装置105で行われる共通の電子透かし方式は、以下の特徴をもつものとする。

(1) 共通の電子透かしは、比較的少ない情報量で耐性の強い電子透かしを実現する。

(2) 共通の電子透かしは、鍵なし又は共通の鍵によって電子透かしを抽出できる。

(3) 共通の電子透かしは、少なくとも各電子透かし方式又はそれを用いて埋め込みを行った機関を特定する情報を埋め込む。

(4) 共通の電子透かしは、各機関の電子透かし埋め込みに対する耐性をもつ。

40

【0023】

上記の特徴をもつ電子透かしとしては種々の方式が考えられるが、耐性の強さをもつ一例として以下の方式を示す。

著作物である入力データを静止画像とした場合、その静止画の画像データを8×8画素のブロックに分割し、そのブロック毎にDCT(Discr eate Cosine Transform: 離散的コサイン変換)を行う。以下、そのDCTしたブロックをDCT係数ブロック、DCT係数ブロックの1係数をDCT係数、1枚の画像のDCT係数ブロックの集合をDCT係数ブロック群と呼ぶものとする。

【0024】

図7(a)は上記透かし埋込装置を示し、図7(b)は上記透かし抽出装置を示す。

50

(a)の透かし埋込装置において、入力画像xを画像変換器701によりDCT変換し、その出力であるDCT係数ブロック群を電子透かし埋め込み器702の入力として用いる。電子透かし埋め込み器702では、入力されたDCT係数ブロック群の中で、埋め込むDCT係数ブロックを1つ選択し、そのDCT係数ブロック中の1つのDCT係数を量子化することによって、1ビットの埋め込みビットを埋め込む。

この時の、量子化ステップの大きさが埋め込みの強度を決定し、その量子化ステップの大きさと選択したDCT係数の位置が鍵情報に対応する。

【0025】

例として、座標u, vの位置にあるDCT係数の値を $s\{u, v\}$ 、量子化ステップをhと表わし、以下に示すような規則により、電子透かしビットの0又は1を埋め込む。

$$a \cdot h < s\{u, v\} \quad (a+1) \cdot h \dots \dots \dots (1)$$

となるaを求める。

【0026】

埋め込みビット=0の時 $c\{u, v\} = b \cdot h + h/2$ (bはa又はa+1の偶数の方) $\dots \dots \dots (2)$

埋め込みビット=1の時 $c\{u, v\} = b \cdot h + h/2$ (bはa又はa+1の奇数の方) $\dots \dots \dots (3)$

となる操作を行い、 $c\{u, v\}$ を埋め込み後の係数とする。

【0027】

最後に、そのブロック群を逆変換器703を用いてIDCT(Inverse DCT: 逆DCT)を行って、8×8画素のブロックに戻し、それを再構成する。これによって、電子透かしが埋め込まれた画像yが得られる。

【0028】

電子透かしの抽出を行う場合は、図7(b)の透かし抽出装置において、上記画像yを上記画像変換器701に入力して、同様のDCTをしたDCT係数ブロック群から電子透かし抽出器705により、鍵情報を用いて埋め込んだDCT係数を選択し、

$$b \cdot h < c\{u, v\} \quad (b+1) \cdot h \dots \dots \dots (4)$$

となるbを求め、bが偶数ならば埋め込みビットは0と判断し、奇数ならば1と判断する。

【0029】

この埋め込み方式において耐性を強化するには以下の手法が考えられる。

DCT係数ブロックの中から埋め込みを行う1つのDCT係数を選択するときに、低周波成分を表わすDCT係数を選べば耐性を強くすることができる。これは、高周波成分が画像圧縮や種々のフィルタリング処理によって失われやすいのに対して、低周波成分は失われにくいためである。

【0030】

また、上記の埋め込み方式では選択するDCT係数ブロック、及び埋め込むDCT係数を1つとして説明したが、その数を増すことによって耐性を強くすることができる。これは、1ビットに対して1つのDCT係数に埋め込んだのみであると、画像圧縮や種々のフィルタリング処理によってその値が失われる可能性が大きい、複数のDCT係数に同じビットを埋め込んでおけば、その大半が失われる可能性が少なくなるためである。

【0031】

また、埋め込むビット自体を誤り訂正符号化することによっても耐性を強くすることができる。これは、埋め込みビットのいくつかが失われても誤り訂正符号によって復元されるためである。ここで、用いる誤り訂正符号の訂正能力が高ければ高いほど耐性が強くなるのは明らかである。ただし、これらの手法は耐性を強くするが、画像の低周波成分を変化させたり、多くのビットを埋め込むために画像の品質が劣化する。また、多くのDCT係数を用いて同じビットを埋め込むために、埋め込めるビットは少なくなることが多い。また、逆の操作を行えば、耐性は弱くなるが、画質が良く、埋め込める情報量も多い電子透かし手法が実現できる。

10

20

30

40

50

【 0 0 3 2 】

以上のような耐性を強化する手法は、DCTを用いる手法に限らず、ウェーブレット変換やフーリエ変換を用いる手法や、直接画素の輝度値などを操作する手法に対しても同じ傾向をもつと言える。

【 0 0 3 3 】

次に、図1を参照して埋め込み手順を説明する。ここでは、共通の電子透かし方式によって埋め込む情報を、簡単のために00、01、10、11とし、各機関101～104を特定する2ビットの情報とするが、他の情報を設定することもできることは明らかである。

【 0 0 3 4 】

各機関101～104は、CD-ROMやフレキシブルディスク、メモ리카ードなどの記憶媒体や、インターネットのようなネットワーク110などの通信媒体を介して配布されるデータに対して上記(1)～(4)の特徴をもつ耐性の強い共通透かし埋込装置105を用いて自機関に対応するビットを埋め込む。その後各機関独自のA～D透かし埋込装置106～109を用いて他の情報を埋め込む。また、ある機関の電子透かし方法と共通の電子透かし方法とが干渉し合わない、即ち、電子透かし埋め込み処理によって共通の電子透かし情報に影響を与えない手法であれば、埋め込み順序は逆にすることもできる。また、各機関毎に埋め込む情報は異なっても良いし、同じ情報でも良い。各機関毎に埋め込む情報としては、著作権情報や利用者情報及び識別情報など種々の情報であることが考えられる。

【 0 0 3 5 】

図2は第1の実施の形態のうちの電子透かしの抽出に関する部分を示す。

図2において、200は統一的な1つの監視機関であり、201～204は図1の各機関101～104に対応する各機関毎の電子透かし監視機関である。統一監視機関200は、図1の共通透かし埋込装置105に対応する共通透かし抽出装置205を有し、各機関201～204は図1のA～D透かし埋込装置106～109に対応する各電子透かし方式によるA～D透かし抽出装置206～209を有している。210は各機関201～204をつなぐネットワークであり、図示はしないが各機関201～204は、このネットワーク210に接続する通信手段を有している。このネットワーク210は図1のネットワーク110と同じものでもよい。

【 0 0 3 6 】

以下、図2における電子透かしの抽出手順を説明する。

統一的な機関200は、CD-ROMやフレキシブルディスク、メモ리카ードなどの記憶媒体や、インターネットのようなネットワーク210などの通信媒体を介して配布され、ネットワーク210上で流通又は利用されているデータの監視を行う。ネットワーク210上で不正コピーと思われるデータが発見又は通報された場合は、共通透かし抽出器205を用いて共通の電子透かしによる埋め込み情報を抽出する。これによって、埋め込みを行った機関又は方法を特定し、そのデータを特定された機関に送る。

【 0 0 3 7 】

データを送られた機関は、各機関独自の電子透かし方式のA～D透かし抽出装置206～209を用いて埋め込んだ種々の情報を抽出する。

【 0 0 3 8 】

本実施の形態によれば、異なる電子透かし方式が混在して用いられるシステムにおいても、各監視機関は多くの方式による電子透かしの埋込部や抽出部を準備することなく、自分の電子透かし方式による埋込部や抽出部のみを管理すればよく、効率的に不正コピーの監視を実現することができる。

【 0 0 3 9 】

また、透かしが発見できなかった場合の安全性も以下の理由により向上できる。即ち、埋め込んだ透かし情報が発見できなかった場合、そのデータには始めから透かし情報がなかったのか、他の方式によって透かしが埋め込まれているのか、透かし情報が攻撃によって

10

20

30

40

50

破壊されたのかを区別することは困難である。しかし、共通の電子透かし方式は耐性が強いので、透かし情報を攻撃によって破壊することは困難である。

【 0 0 4 0 】

従って、最初の手順によって共通の電子透かしによる透かし情報が抽出された場合、始めから透かし情報が入っていなかった可能性は排除される。次に、各機関独自の電子透かし方式は任意であるが、詳細情報を埋め込む場合、埋め込む情報量が多くなり品質劣化の抑制を重視した比較的耐性の弱い電子透かし方式となる場合が多い。従って、共通の電子透かし方式による透かし情報の抽出後に各機関独自の電子透かし方式による透かし情報が抽出できない場合は、攻撃による電子透かし情報の破壊であると言える。

【 0 0 4 1 】

よって、このシステムによって各機関が単独に独自電子透かし方法を用いるよりも全体的な安全性が向上していることが言える。

尚、本実施の形態では4つの機関からなる例について説明したが、任意の数の機関に対しても同様に実施できることは明らかである。

【 0 0 4 2 】

(第 2 の実施の形態)

図 3 は、本発明の第 2 の実施の形態による情報処理システムにおける電子透かしの埋め込みに関する部分を示す。本実施の形態は、共通透かし埋込装置 1 0 5 による埋め込みを、共通埋め込み機関 3 0 0 のみが行う場合である。

3 0 1 ~ 3 0 4 は、図 1 の各機関 1 0 1 ~ 1 0 4 からそれぞれ共通透かし埋込装置 1 0 5 を除いた独自の電子透かし方式による A ~ D 透かし埋込装置 1 0 6 ~ 1 0 9 のみをもつ各機関であり、1 1 0 はネットワークである。

【 0 0 4 3 】

尚、共通埋め込み機関 3 0 0 としては、音楽著作物に対する J A S R A C のような統一的な著作権管理機関が考えられ、各機関 3 0 1 ~ 3 0 4 としては、共通埋め込み機関 3 0 0 によって管理されている著作物をユーザに販売する販売店のような形態が考えられるが、本実施の形態で特定するものではなく、共通で耐性の強い電子透かし方式と各機関独自の電子透かし方式とを用途に応じて使い分ける手法は全て本発明に含まれる。

【 0 0 4 4 】

この場合は各機関 3 0 1 ~ 3 0 4 (個々の著作者を含む) は、著作物を機関 3 0 0 に登録し、共通透かし埋込装置 1 0 5 による埋め込みを依頼する。機関 3 0 0 は共通の電子透かし方式によって所定の情報を埋め込み、各機関 3 0 1 ~ 3 0 4 に返信する。各機関 3 0 1 ~ 3 0 4 は、それぞれ独自の電子透かし方式による A ~ D 埋込装置 1 0 6 ~ 1 0 9 を用いて種々の情報を埋め込む。

【 0 0 4 5 】

本実施の形態の第 1 の実施の形態に対する利点は次の通りである。

第 1 の実施の形態では、各機関が共通の電子透かし方式による埋め込みを行うために、共通の電子透かし方式、及びその鍵は各機関に公開されている必要がある。安全性のためには共通の電子透かし方式及び鍵は秘密にした方が良いが、各機関の内の 1 つでもその秘密を守れなければ全体の安全性が保持できない。しかし、本実施の形態では、共通の電子透かし方式を各機関 3 0 1 ~ 3 0 4 に公開する必要がないので安全性が向上する。

【 0 0 4 6 】

また、第 1 の実施の形態と融合した形態も考えられる。例えば、図 3 において機関 3 0 1 と 3 0 2 は第 1 の実施の形態と同様に共通透かし埋込装置 1 0 5 をもつものとする。この場合、共通透かし埋込装置 1 0 5 を持たない機関 3 0 3 と 3 0 4 は本実施の形態と同様の処理を行うが、共通透かし埋込装置 1 0 5 をもつ機関 1 0 1 と 1 0 2 は共通の電子透かし方式による所定情報の埋め込みを第 1 の実施の形態のように自機関内で行うことができる。

【 0 0 4 7 】

図 4 は第 2 の実施形態による情報処理システムにおける電子透かしの抽出に関する部分を

10

20

30

40

50

示す。

図4において、400は統一的な1つの監視機関であり、共通透かし埋込装置105に対応する共通抽出装置205と、各機関独自の電子透かし方式によるA～D埋込装置106～109に対応するA～D抽出装置206～209を有する。210はネットワークである。尚、図示していないが図1又は図3の各機関101～104又は301～304等がネットワーク210に接続されているものとする。

【0048】

以下、図4における電子透かしの抽出手順を説明する。

機関400は、CD-ROMやフレキシブルディスク、メモ리카ードなどの記憶媒体や、インターネットのようなネットワーク210などの通信媒体を介して配布され、ネットワーク210で流通又は利用されているデータの監視を行う。ネットワーク210上で不正コピーと思われるデータが発見又は通報された場合は、共通透かし抽出装置205を用いて共通の電子透かしによる埋め込み情報を抽出する。これによって、埋め込みを行った機関又は方法を特定する。次に、特定された機関独自の電子透かし方法の抽出装置を用いて埋め込んだ種々の情報を抽出する。

【0049】

本実施の形態によるシステムでは、1つの統一的な監視機関だけで不正コピーの監視が可能である。このような統一的な監視機関は、各機関独自の電子透かし方式が有限であれば実現可能である。また、共通の電子透かし方式によって各機関独自の電子透かし方式が特定されるので、試行錯誤的に各機関独自の電子透かし方式を試す必要がなく効率的である。

【0050】

ただし、統一監視機関は始めから全ての各機関独自の電子透かし方式を準備している必要はなく、共通の電子透かし方式による透かし情報によって埋め込み機関が特定されたときに、その機関に連絡して各機関独自の電子透かし方式の抽出手段及び鍵などを提供してもらうこともできる。

【0051】

(第3の実施の形態)

図5は図1及び図3に対応する電子透かしの抽出に関する部分を示す。

図5において、501～504は共通透かし埋込装置105に対応する共通透かし抽出装置205と、各機関独自の電子透かし方式によるA～D埋込装置106～109に対応するA～D抽出装置206～209を各々有する。

【0052】

以下、図5における電子透かしの抽出手順を説明する。

各機関501～504は、CD-ROMやフレキシブルディスク、メモ리카ードなどの記憶媒体や、インターネットのようなネットワーク210などの通信媒体を介して配布され、ネットワーク210で流通又は利用されているデータの監視を行う。ネットワーク210上で不正コピーと思われるデータが発見又は通報された場合は、共通透かし抽出装置205を用いて共通の電子透かしによる埋め込み情報を抽出する。これによって、埋め込みを行った機関又は方法を特定し、自機関の方法と特定された場合は、自機関独自の透かし抽出装置により抽出を行う。他機関である場合は、状況に応じて通報又は破棄等の処理を行う。

【0053】

本実施の形態によるシステムでは、統一的な監視機関をもたずに不正コピーの監視が可能である。このシステムは図1及び図3のどちらの埋め込みシステムにも対応可能である。また、図2、図4も図1及び図3のどちらの埋め込みシステムにも対応可能であることは明らかである。

【0054】

また、図2、図4、図5を融合した形態も考えられる。例えば、第1の実施の形態の図2において、機関200は第2の実施の形態の機関300のように全てのA～D透かし抽出

10

20

30

40

50

装置をもち、機関 201 と 202 は第 3 の実施の形態と同様に共通透かし抽出装置 205 をもつものとする。この場合、共通透かし抽出装置 205 をもたない機関 203 と 204 は第 1 の実施の形態と同様の処理を行うが、共通透かし抽出装置 205 を持つ機関 300 及び 201 と 202 は共通透かし抽出装置による透かし情報の抽出を第 2、3 の実施の形態のように自機関内で行うことができる。

以上を含めて、共通で耐性の強い電子透かし方式と各機関独自の電子透かし方式を用途に応じて使い分ける手法は全て本発明に含まれる。

【0055】

(第 4 の実施の形態)

図 1、図 3 の埋め込みシステムにおいて、各機関はその埋込装置に対応する抽出装置を有し、埋め込み前に透かし情報の抽出検査を行う形態も可能である。

10

本実施の形態としては、上述の各実施の形態及びその組み合わせが考えられるが、ここでは図 3 に示した形態を例に図 6 を参照して説明を行う。

図 6 において、600 は共通の埋め込み機関であり、共通透かし埋込装置 105 と、それに対応する共通透かし抽出装置 205 を有する。601 ~ 604 は各機関独自の電子透かし方式による A ~ D 透かし埋込装置 106 ~ 109 と、それに対応する A ~ D 透かし抽出装置 206 ~ 209 を有する機関である。

【0056】

各機関 601 ~ 604 (個々の著作権を含む) は著作物を機関 600 に登録し、共通透かし埋込装置 105 による埋め込みを依頼する。機関 600 は、共通透かし埋込装置 105 を用いる前に、共通透かし抽出装置 205 を用いてその著作物が不正コピーでないことを確認する。例えば、共通透かし抽出装置 205 によってその著作物に既に共通の電子透かしが埋め込まれていることが分かった場合は、依頼元又は透かし情報によって特定された機関に確認を行う。問題がなければ共通透かし埋込装置 105 によって所定の情報を埋め込み依頼元に返信する。依頼元は各機関独自の埋込装置 106 ~ 109 を用いて種々の情報を埋め込む。

20

【0057】

本実施の形態によるシステムによれば、依頼者の不正申告による電子透かしの上書きなどを防ぐことができる。また、埋め込み機関と抽出機関を同じにして効率的なシステムを実現することもできる。

30

【0058】

次に、本発明の他の実施の形態としての記憶媒体について説明する。

本発明は上記各実施の形態で説明したシステムや装置を組み合わせで行う場合のみに限定されるものではなく、上記システム又は装置内のコンピュータ (CPU あるいは MPU) に、上記各実施の形態を実現するためのソフトウェアのプログラムコードを供給し、このプログラムコードに従って上記システムあるいは装置のコンピュータが上記各種デバイスを動作させることにより、上記各実施の形態を実現する場合も本発明の範疇に含まれる。

【0059】

またこの場合、上記ソフトウェアのプログラムコード自体が上記各実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、具体的には上記プログラムコードを格納した記憶媒体は本発明の範疇に含まれる。

40

【0060】

このようなプログラムコードを格納する記憶媒体としては、例えば ROM、RAM 等の半導体メモリ、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性メモリカード、を用いることができる。

【0061】

また、上記コンピュータが、供給されたプログラムコードのみに従って各種デバイスを制御することにより、上記各実施の形態の機能が実現される場合だけではなく、上記プログラムコードがコンピュータ上で稼働している OS (オペレーティングシステム)、あるいは

50

は他のアプリケーションソフト等と共同して上記各実施の形態が実現される場合にも、かかるプログラムコードは本発明の範疇に含まれる。

【0062】

さらに、プログラムがコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能格納ユニットに備わるCPU等が実際の処理の一部又は全部を行い、その処理によって上記各実施の形態が実現される場合も本発明の範疇に含まれる。上述の実施の形態によれば、異なる電子方式が混在して用いられるシステムにおいても、監視機関は多くの電子透かしの埋込装置や抽出装置を準備することなく、効率的に不正コピーを監視することができる。また、電子透かしが発見できなかった場合の安全性も各電子透かし方式単独に用いるよりも向上させることができる。

10

【0063】

【発明の効果】

以上説明した通り、本発明によれば、各機関に独自の電子透かしの方式を示す情報をデジタルデータに埋め込むために利用される共通の電子透かし方式について、各機関に公開する必要がなくなるので、安全性が向上する。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態による情報処理システムにおける電子透かしの埋め込みに関する部分を示すブロック図である。

【図2】本発明の第1の実施の形態による情報処理システムにおける電子透かしの抽出に関する部分を示すブロック図である。

20

【図3】本発明の第2の実施の形態による情報処理システムにおける電子透かしの埋め込みに関する部分を示すブロック図である。

【図4】本発明の第2の実施の形態による情報処理システムにおける電子透かしの抽出に関する部分を示すブロック図である。

【図5】本発明の第3の実施の形態による情報処理システムにおける電子透かしの抽出に関する部分を示すブロック図である。

【図6】本発明の第4の実施の形態による情報処理システムにおける電子透かしの埋め込みと抽出に関する部分を示すブロック図である。

【図7】電子透かしの埋込装置及び抽出装置を示すブロック図である。

30

【符号の説明】

101～104 監視機関

106～109 A～D透かし埋込装置

110 ネットワーク

200 統一的な監視機関

201～204 監視機関

205 共通透かし抽出装置

206～209 A～D透かし抽出装置

210 ネットワーク

300 共通埋め込み機関

40

301～304 監視機関

400 統一的な監視機関

501～504 監視機関

600 共通埋め込み機関

601～604 監視機関

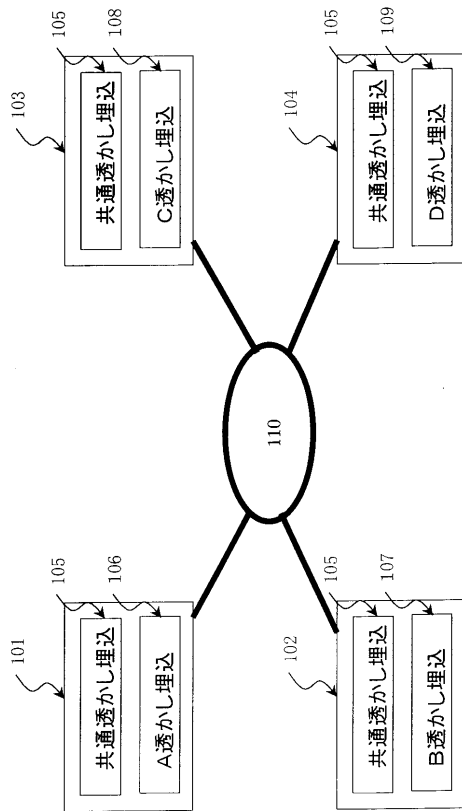
701 画像変換器

702 電子透かし埋め込み器

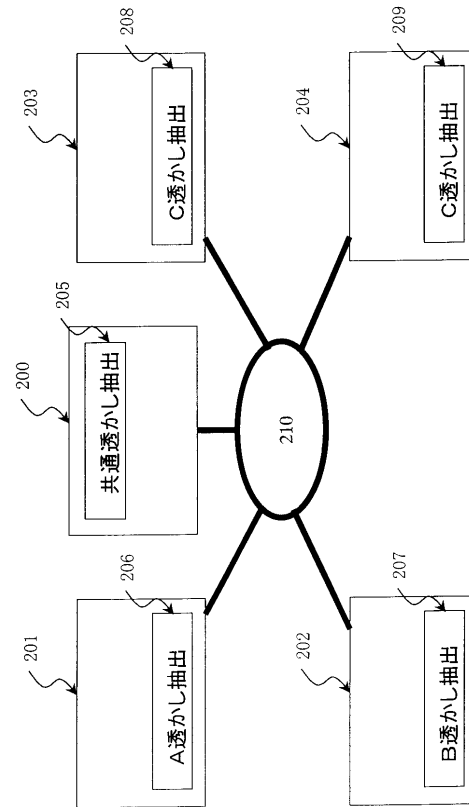
703 画像逆変換器

705 電子透かし抽出器

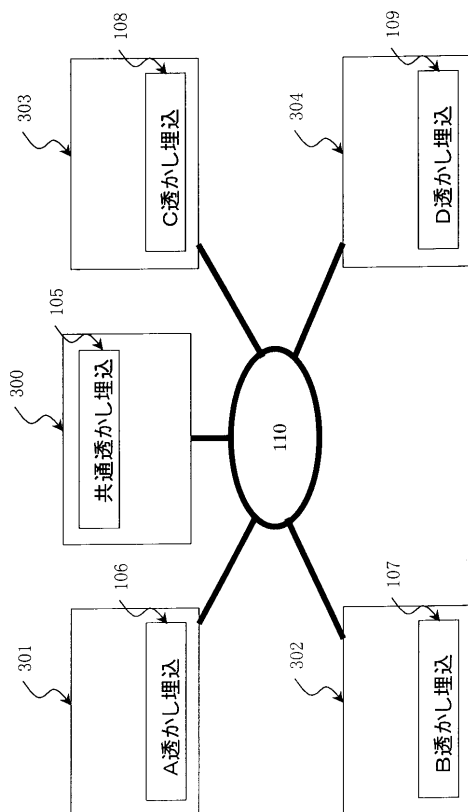
【図 1】



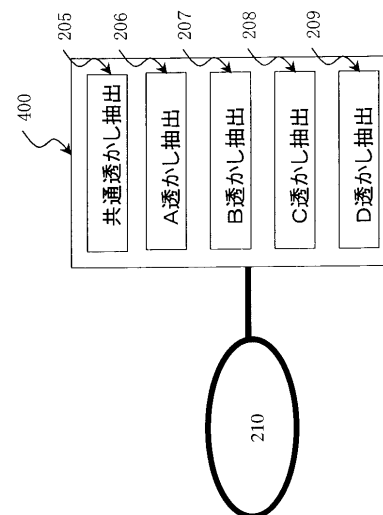
【図 2】



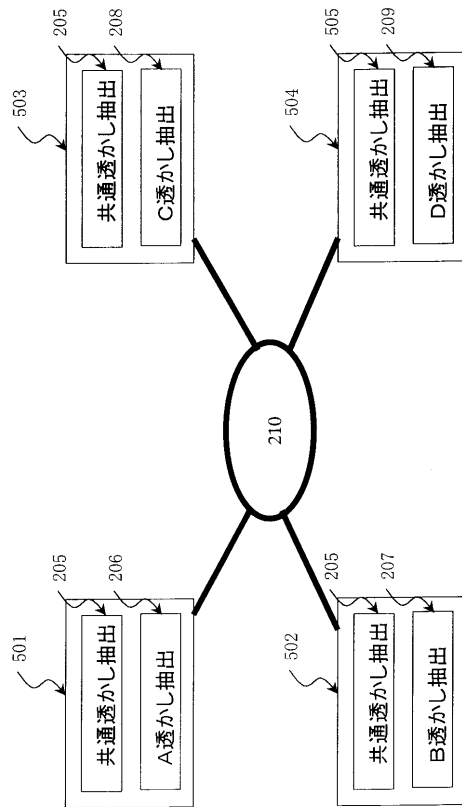
【図 3】



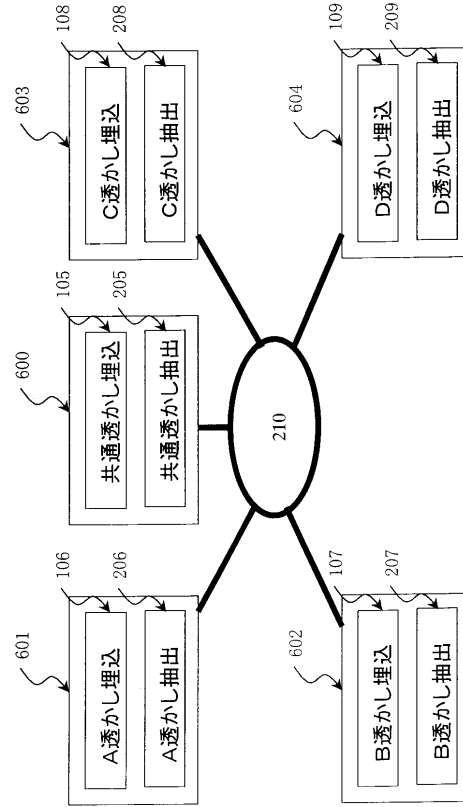
【図 4】



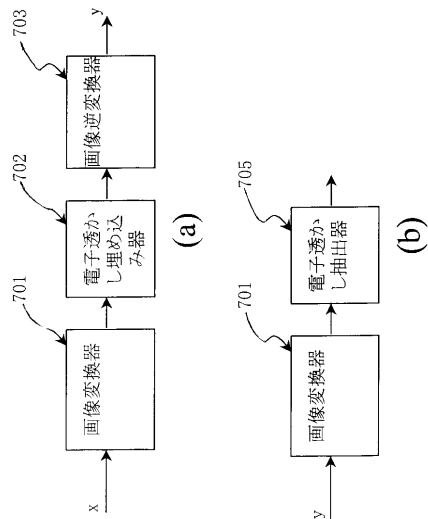
【図 5】



【図 6】



【図 7】



フロントページの続き

(58)調査した分野(Int.Cl. , D B 名)

H04N 1/38- 1/393

G06T 1/00