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

特許第4889274号
(P4889274)

(45)発行日　平成24年3月7日(2012.3.7)　(24)登録日　平成23年12月22日(2011.12.22)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675B
G09C	1/00	(2006.01)	G09C	1/00	640D

請求項の数 8　外国語出願　(全 17 頁)

(21)出願番号	特願2005-295204 (P2005-295204)
(22)出願日	平成17年10月7日 (2005.10.7)
(65)公開番号	特開2006-115501 (P2006-115501A)
(43)公開日	平成18年4月27日 (2006.4.27)
審査請求日	平成20年10月7日 (2008.10.7)
(31)優先権主張番号	10/963,696
(32)優先日	平成16年10月13日 (2004.10.13)
(33)優先権主張国	米国 (US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ビン　チュー
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】離散レベル改ざん位置同定による安全画像認証

(57)【特許請求の範囲】

【請求項１】

マルチメディアの真正性を決定するために、データブロックにより、前記マルチメディアを評価するステップと、

前記マルチメディアが真正でないとの決定に応答して、前記マルチメディアの改ざん部分を位置同定するステップとを備え、

前記位置同定するステップは、

障害のある画像をシャッフリングして、ランダム化された近傍データを有するシャッフル画像を生成するステップと、

前記シャッフル画像、および改ざんされたピクセルまたはサンプルを検出する署名手順において署名すべき前記マルチメディアに埋め込まれた原ロゴ画像を、低次元ベクトルに変換するステップと、

前記障害のある画像に対応する前記低次元ベクトルの１つの低次元ベクトルから、埋め込みロゴを抽出するステップと、

前記抽出された埋め込みロゴを前記原ロゴと比較して、不一致のピクセルまたはサンプルを識別するステップと、

先に適用された次元低減動作を逆にすることによって、前記低次元ベクトルをスキャンして高次元ベクトルにするステップと、

前記シャッフリング動作を逆転させて、前記シャッフル画像における不一致のピクセルまたはサンプルに対応する前記マルチメディアの特定のピクセルまたはサンプルを位置

同定するステップと
を含み、前記特定のピクセルまたはサンプルは、改ざんされたピクセルまたはサンプルであることを特徴とする方法。
【請求項２】
前記データブロックは、画像またはビデオデータのピクセルブロックであり、前記改ざん部分は、１つまたは複数のピクセルであるか、または前記データブロックは、音声データのサンプルブロックであり、前記改ざん部分は、１つまたは複数のサンプルであることを特徴とする請求項１に記載の方法。
【請求項３】
前記マルチメディアを評価するステップは、
埋め込みのために選択される１組のピクセルまたはサンプルの最下位ビット（ＬＳＢ；ｌｅａｓｔ　ｓｉｇｎｉｆｉｃａｎｔ　ｂｉｔ）から、ディジタル署名、キー付きハッシュ、またはＭＡＣを含んでいるデータを前記マルチメディアから抽出するステップと、
前記データがディジタル署名である場合には、前記データを使用して前記マルチメディアを暗号解読し、ディジタル署名が使用されている場合に、第１のハッシュ値を取得するステップと、
前記データがキー付きハッシュもしくはＭＡＣの場合には、前記キー付きハッシュもしくはＭＡＣが第１のハッシュ値であり、マルチメディアを認証署名するのに使用するのと同様の動作によって決定される、複数の分離された部分区間に属する特定の分離された部分空間のＬＳＢをゼロにするステップと、
前記分離された部分空間のビットをハッシングして、第２のハッシュ値を取得するステップと、
前記第１のハッシュ値を前記第２のハッシュ値と比較するステップと、
前記比較するステップに応答して、前記第１のハッシュ値と前記第２のハッシュ値が一致する場合は前記マルチメディアが真正であると決定し、そうでない場合には真正でないと決定するステップと
を含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記位置同定するステップは、
前記抽出されたロゴと前記原ロゴとの間の不一致のピクセルまたはサンプルに対応する改ざんされたピクセルまたはサンプルを拡張して、前記不一致のピクセルまたはサンプルの場所において、各個別ピクセルまたはサンプルに署名するのに使用される、それぞれの近傍ピクセルまたはサンプルを含めるステップと、
前記改ざんされたピクセルまたはサンプルの拡張された組の真正でないピクセルまたはサンプルを、事前設定の閾値よりも大きな接続経路を有するピクセルまたはサンプルとして識別するステップと
を含んでいる、ピクセルまたはサンプル近傍依存性基準の関数として前記改ざんされたピクセルまたはサンプルを再評価するステップを含むことを特徴とする請求項１に記載の方法。
【請求項５】
前記マルチメディアは、秘密に選択されたピクセル内に埋め込まれるディジタル署名、キー付きハッシュ、またはＭＡＣを含み、前記マルチメディアの真正性を決定するために、前記マルチメディアを評価するステップは、
前記ディジタル署名、キー付きハッシュ、またはＭＡＣを、前記選択されたピクセルから抽出するステップと、
前記ディジタル署名が使用されている場合には、暗号解読して第１のハッシュ値を回復するステップと、
前記キー付きハッシュもしくはＭＡＣが使用されている場合には、前記キー付きハッシュもしくはＭＡＣが第１のハッシュ値であり、前記マルチメディアを認証署名するのに使用するのと同様の動作によって決定される、複数の分離された部分区間に属する特定の分

離された部分空間の特定のビットをゼロにするステップと、
前記分離された部分空間のビットをハッシングして、第２のハッシュ値を取得するステップと、
前記第１のハッシュ値を前記第２のハッシュ値と比較するステップと、
前記比較するステップに応答して、前記第１のハッシュ値と前記第２のハッシュ値が一致する場合は前記マルチメディアが真正であると決定し、そうでない場合には真正でないと決定するステップと
を含むことを特徴とする請求項１に記載の方法。
【請求項６】
前記評価するステップおよび前記位置同定するステップの前に、真正性検証のために前記マルチメディアにダイジェストを埋め込むステップをさらに備えたことを特徴とする請求項１に記載の方法。
【請求項７】
請求項１乃至６のいずれかに記載の方法をコンピュータに実行させるコンピュータプログラム命令を記憶したコンピュータ読取可能な記憶媒体。
【請求項８】
プロセッサと、
請求項１乃至６のいずれかに記載の方法をコンピュータ装置に実行させるコンピュータプログラム命令を記憶し、前記プロセッサに結合されたメモリと
を備えたコンピュータ装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般には、マルチメディア認証、および改ざんされたピクセルまたはサンプルの位置同定に関し、より詳細には、離散レベル改ざん位置同定による安全画像認証に関する。
【背景技術】
【０００２】
マルチメディア認証は、マルチメディア信号の真正性（ａｕｔｈｅｎｔｉｃｉｔｙ）および完全性を検査する技術である。改ざんされた信号に対して、改ざんされたピクセルまたはサンプルの位置同定をして（ｌｏｃａｌｉｚｅ）、未修正の部分を使用できるようにすることが望ましいことが多い。この目標を達成する技術が、近年においてさかんに研究された。完全認証またはハード認証（ｈａｒｄ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ）と呼ばれる、提案技術の部類は、マルチメディア信号に対するなんらかの修正を検出するものである。ハード認証技術は、ピクセルワイズスキーム（ｐｉｘｅｌ－ｗｉｓｅ　ｓｃｈｅｍｅ）とブロックワイズスキーム（ｂｌｏｃｋ－ｗｉｓｅ　ｓｃｈｅｍｅ）に分類することができる。ピクセルワイズスキームは、信号全体に対する真正性の検証に加えて、改ざんされたピクセル（または、以下においては、音声信号に対する明示的な参照のない「ピクセル」が意味する、サンプル）を位置同定するように設計されている。他方、ブロックワイズスキームは、改ざんブロックを位置同定するように設計される。ブロックワイズスキームは一般にピクセルワイズスキームより安全性が高いが、その改ざん位置同定能力はずっと粗い。提案の認証技術についての詳細は文献に記載されている（非特許文献１、２）。
【０００３】
最初のピクセルワイズ認証法の１つは、ＹｅｕｎｇとＭｉｎｔｚｅｒによって提案された弱い電子透かし法（ｆｒａｇｉｌｅ　ｗａｔｅｒｍａｒｋｉｎｇ　ｓｃｈｅｍｅ）である（Ｙ－Ｍ法）（非特許文献３、４）。グレースケール画像に対しては、Ｙ－Ｍ法では、秘密２値関数を適用して、必要ならばパータベーションを加えた（ｐｅｒｔｕｒｂ）、各ピクセルの値を事前設定ロゴビット（ｐｒｅｓｅｔ　ｌｏｇｏ　ｂｉｔ）にマッピングする。このスキームは、単一の改ざんされたピクセルを位置同定することができる。このス

キームの様々な環境下での脆弱性（ｖｕｌｎｅｒａｂｉｌｉｔｙ）についての報告（非特許文献５～９）、および対応処置（ｆｉｘ）についての報告がある（非特許文献１０～１３）。代表的な対応処置としては、ピクセルをロゴビットにマッピングする際に近傍依存性（ｎｅｉｇｈｂｏｒｈｏｏｄ　ｄｅｐｅｎｄｅｎｃｙ）を導入するものがある（非特許文献１０）。これらの対応処置は、前記文献（非特許文献５～９）に報告されている攻撃を阻止することができるが、Ｆｒｉｄｒｉｃｈによって指摘されているように（非特許文献１４）、ピクセルスキャン順序、すなわち埋め込みプロセスにおいてピクセルに電子透かしが入れられる順序が公開されている場合で、かつオラクルが検出された改ざんされたピクセルの位置を返す場合には、オラクル攻撃に対して脆弱である。Ｆｒｉｄｒｉｃｈは、この新規の脆弱性は、ピクセルワイズスキームにおける電子透かし処理時のピクセル修正における本質的な順次特性によるものとしており、ピクセルワイズスキームではこのような脆弱性を対応処置できないと考えた。彼女は、その関心をブロックワイズスキームの開発に向け（非特許文献１４）、このスキームは、前述したピクセルワイズスキームに対する脆弱性のいずれにも煩わされることがない。不運なことに、ブロックワイズスキームは、改ざん位置同定能力を大幅に低下させる。改ざんされたピクセルを識別することはできなくなる。

【０００４】

さらに、すべての既存ピクセルワイズスキームは、ピクセルスキャン順序が公開であるか、または秘密（（ｐｒｉｖａｔｅ／ｓｅｃｒｅｔ）であるかにかかわらず、オラクル攻撃に対して脆弱である。そのようなスキームでは、通常、改ざんされたピクセルがない場合には、画像は真正であると断言する。そのようなスキームにおいては、ピクセルの真正性は、各ピクセルの値をロゴビットと比較されるビットにマッピングする、多対一（ｍａｎｙ－ｔｏ－ｏｎｅ）マッピング関数を適用することによって検査される。ピクセルは、一時に１ピクセルずつ、連続して電子透かしが入れられる。これらの機能によって、ピクセルワイズスキームでは良好な認知品質（ｐｅｒｃｅｐｔｕａｌ　ｑｕａｌｉｔｙ）が得られるが、オラクル攻撃にはやはりつけこまれる（参照により本明細書に組み入れた、非特許文献１５を参照）。

【０００５】

上記の観点から、一般的には、ブロックワイズ画像認証スキームが唯一の実行可能な解決策であると考えられる。そのような解決策の１つが、単一ピクセルではなく改ざんされたブロックを位置同定することのできる、ブロックワイズ認証スキームである。安全性上の理由から、ブロックの大きさは一般に１２８ピクセル以上である。

【０００６】

（参考文献）

以下の文献を背景技術において使用する。

【０００７】

【非特許文献１】B.B.Zhu, M.D.Swanson, and A.H.Tewfik, "When Seeing Isn't Believing," IEEE Signal Processing, vol.21, no.2, pp.40-49, March 2004

【非特許文献２】B.B.Zhu and M.D.Swanson, "Multimedia Authentication and Watermarking," Multimedia Information Retrieval and Management, D.Feng, W.C.Siu, and H.Zhang, Eds, Springer-Verlag, Berlin, Heidelberg, New York, 2003, chap 7, pp.948-177

【非特許文献３】M.M.Yeung and F.C.Mintzer, "An Invisible Watermarking Technique for Image Verification," IEEE Int Conf Image Processing, 9997, vol.2, pp.680-683

【非特許文献４】M.M.Yeung and F.C.Mintzer, "Invisible Watermarking for Image Verification," J.Electronic Imaging, vol.7, no.3, pp.578-591, July 1998

【非特許文献５】N.Memon, S.Shende, and P.Wong, "On the Security of the Yeung-Mintzer Authentication Watermark," Proc IS&T PICS Symp, Savannah, Georgia, March 1999, pp.301-306

【非特許文献６】J.Fridrich, M.Goljan, and N.Memon, "Further Attacks on Yeung-Min

tzer Fragile Watermarking Scheme," Proc SPIE vol 3971 Security and Watermarking of Multimedia Contents II, San Jose, CA, Jan 2000, pp.428-437
【非特許文献７】M.Holliman and N.Memon, "Counterfeiting Attacks on Oblivious Block-wise Independent Invisible Watermarking Schemes," IEEE Trans Image Processing, vol.9. no.3, March 2000, pp.432-441
【非特許文献８】J.Fridrich, M.Goljan, and N.Memon, "Cryptanalysis of the Yeung-Mintzer Fragile Watermarking Technique," J.Electronic Imaging, vol.91, pp.262-274, 2002
【非特許文献９】J.Wu, B.Zhu, S.Li, and F.Lin, "Efficient Oracle Attacks on Yeung-Mintzer and Variant Authentication Schemes," IEEE Int Conf Multimedia & Expo, Taiwan, Jun 2004
【非特許文献１０】J.Fridrich, M.Goljan, and A.C.Baldoza, "New Fragile Authentication Watermark for Images," IEEE Int Conf Image Processing, Vancouver, Canada, Sept, 2000, vol.9, pp.446-441
【非特許文献１１】C.T.Li, F.M.Yang, and C.S.Lee, "Oblivious Fragile Watermarking Scheme for Image Authentication," IEEE Int Conf Acoustics, Speech, & Signal Processing, Orlando, FL, USA, May 2002, vol VI, pp 3445-3448
【非特許文献１２】H.Zhong, F.Liu, and L.C.Jiao, "A New Fragile Watermarking Technique for Image Authentication," Int Conf Signal Processing, Aug 2002, Beijing, vol.9, pp.792-795
【非特許文献１３】H.Lu, R.Shen, and F.Chung,, "Fragile Watermarking Scheme for Image Authentication," Electronics Letters, vol.39, no.12, June 2003, pp.898-100
【非特許文献１４】J.Fridrich, "Security of fragile authentication watermarks with localization," Proc SPIE vol.4675, Security and Watermarking of Multimedia Contents IV, Jan 2002, pp.691-700
【非特許文献１５】Jinhai We et al, "Efficient Oracle Attacks on Yeung-Mintzer and Variant Authentication Schemes", June 2004.

【発明の開示】
【発明が解決しようとする課題】
【０００８】
ブロックワイズスキームは、オラクル攻撃に対して脆弱でない唯一の画像認証技法であると考えられるが、多くの用途では、より精細な改ざん位置同定能力を有する認証スキームの恩恵がある。不運なことに、上述したように、既存のピクセルワイズスキームは、ピクセルスキャン順序が公開であるか秘密であるかにかかわらず、オラクル攻撃の下では脆弱である。
【課題を解決するための手段】
【０００９】
離散レベル改ざん位置同定による、安全マルチメディア認証のためのシステムおよび方法について記述する。これらの観点において、「離散（ｄｉｓｃｒｅｔｅ）」の用語は、改ざん位置同定が、画像またはビデオデータに対してピクセルレベルであるか、または音声データに対してサンプルレベルであることを意味する。より具体的には、一観点において、マルチメディアが評価されて、そのマルチメディアの真正性が決定される。この評価は、データブロックに基づいている。そのマルチメディアが真正でないとの決定に応じて、マルチメディアの改ざん部分が、改ざん部分の各々のピクセルまたはサンプルをアドレス指定することによって、位置同定される。
【００１０】
図において、構成要素の参照符号の左端桁は、その構成要素が最初に現れる特定の図を識別する。
【発明を実施するための最良の形態】
【００１１】

（例示的システム）
図１は、離散的改ざん位置同定による安全画像認証の例示的システム１００を示す。システム１００は、コンピュータ装置１０２を含み、このコンピュータ装置は、プログラムモジュール１０４およびプログラムデータ１０６を含む。プログラムモジュール１０４は、例えば、画像認証モジュール１０８を含み、このモジュールは、離散的改ざん位置同定による安全画像認証を実行する。プログラムデータ１０６は、例えば、画像１１０、真正および／または改ざん画像指示１１２、改ざんされたピクセル１１４、およびその他のデータ１１６を含む。

【００１２】
画像認証モジュール１０８は、信号真正性検証１１８機構および改ざんされたピクセル位置同定１２０機構を含む、２重の独立する機構で画像１１０を確実に認証する認証スキームを提供する。これらの統合はされているが、独立した機構によって、ピクセルワイズスキームとブロックワイズスキームの最善部分が単一システムに結合されて、すべての既知の攻撃に対して安全であり、同時に離散的改ざん位置同定を維持する、離散的改ざん位置同定機能による安全認証スキームが得られる。信号真正性検証１１８および改ざんされたピクセル位置同定１２０は、各々のタスクについて最適化される。このことは、真正性検証と改ざん位置同定という２つのまったく異なる目的に対して単一の機構を利用するために脆弱性がある、既存のピクセルワイズスキームと対照的である。

【００１３】
より具体的には、信号真正性検証１１８では、画像１１０の真正性を検証するためにブロックワイズスキームを実現する。一実現形態においては、画像全体１１０がブロックと考えられる。別の実現形態においては、画像１１０は、複数の切り離されたブロックにセグメント化されて、ブロックワイズスキームが各ブロックに適用される。改ざんされたピクセル位置同定１２０は、信号真正性検証１１８と統合されて、改ざんされたピクセルを位置同定するピクセルワイズ機構を提供する。このピクセルワイズ機構は、画像１１０内の各ピクセルを個別にアドレス指定してピクセルレベル改ざん位置同定をもたらす。これは、信号真正性検証１１８におけるブロックワイズスキームとは異なるものであり、ブロックワイズスキームでは、ブロック全体、すなわちピクセルの集まりに対して状態を指示する出力（真正性ありまたはなし）が生成され、したがってブロック内の各ピクセルに対する状態を指示することはできない。改ざんされたピクセル位置同定１２０では、ピクセルスキャン順序において、１つまたは複数の先に電子透かしを入れたピクセルを、現在ピクセルの近傍として利用する。画像内でピクセルを順序づける任意の方法を、ピクセルスキャン順序として使用することができる。このスキャン順序は、公的に開示することも、秘密の情報として維持することもできる。以下に説明する特定の実現形態においては、ピクセルのランダム順序化を、ピクセルスキャン順序として使用する。以下に説明するように、このピクセルのランダム順序化によって、改ざんされたピクセルの候補を絞り込む事後処理が可能となり、したがって画像１１０の単一の改ざんされたピクセルさえも検出する確率が改善される。ピクセルのランダム順序化を生成する方法については、本稿で後ほど述べる。

【００１４】
この実現形態においては、考察および例示的応用の目的で、画像１１０はＬビットグレースケール画像１１０、Ｌ＞１であるが、記述する画像真正性検証モジュール１０８の動作は、カラー画像または音声またはビデオデータなどのマルチメディアタイプについても可能である。例えば、カラー画像に対しては、グレースケール画像に対する画像真正性モジュール１０８ハッシュ動作を、全カラー成分に適用することができる。結果として得られるディジタル署名を、Ｙ成分などの１つのカラー成分に埋め込み、同時にグレースケール画像に対する改ざんされたピクセル位置同定１２０の動作を、各カラー成分に独立に適用することができる。カラー画像に対する代替実現形態は、グレースケール画像に対する画像認証モジュール１０８の動作を、各カラー成分に独立に適用することである。この場合には、信号真正性検証１１８は、各カラー成分に対して真正性を検証することができる

。

【００１５】

（例示的画像署名手順）

改ざんされたピクセル位置同定１２０は、弱い電子透かしを画像１１０に埋め込むことによって、電子透かし動作を実現する。弱い電子透かしは、特殊な種類の電子透かしであり、電子透かしを入れた信号が小さな変化をすると、その完全性が破壊される。この電子透かしを、改ざんされたピクセルを検出／位置同定するのに使用する。信号真正性検証１１８は、ディジタル署名またはＭＡＣ（メッセージ認証コード（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ））を生成する。説明の目的で、このディジタル署名またはＭＡＣは、「その他データ」１１６の各々の部分として示してある。電子透かし処理構成要素１２２は、最下位ビット埋め込み（電子透かし処理）を使用して、ディジタル署名またはＭＡＣを、場合によっては画像ＩＤ、画像サイズ、題目、所有者情報、その他などの任意選択の埋め込みデータと共に、画像１１０の選択されたピクセル中に埋め込む。また、電子透かし構成要素は、電子透かし処理画像１１０から、電子透かしおよびことによるとその他のデータを抽出する。

【００１６】

図２は、グレースケール画像１１０に署名する手順２００の例示的動作を示す。考察の目的で、この手順の観点を、図１の機能に関して考察する。構成要素参照番号の最左端桁は、その構成要素が最初に現れる特定の図を識別する。ブロック２０２において、画像認証モジュール１０８は、グレースケール画像Ｉ１１０に対して選択された秘密キー（ｓｅｃｒｅｔ　ｋｅｙ）Ｋを使用して、ランダムマッピング関数ｆを生成する。「秘密」という用語は、キーを秘密として維持されなくてはならないことを意味する。この「秘密キー」Ｋの用語は、公開／秘密暗号化暗号における「秘密鍵（ｐｒｉｖａｔｅ　ｋｅｙ）」とは異なり、この秘密鍵も本明細書のいくつかの実現形態においては使用する。秘密キーＫは、ユーザが選択して、モジュール１０８に入力する。ランダムマッピング関数ｆは、［０，$2^{L}-1$］の範囲の整数、すなわちピクセル値を、バイナリ値ｆ（ｘ）＝ｂ、$\forall x \in$［０，$2^{L}-1$］にマッピングし、ここでｂは１または０である。一実現形態においては、キーＫは画像Ｉから分離して維持される。代替的な一実現形態においては、Ｋは暗号化されて、画像１１０のヘッダーに挿入されるか、または電子透かし処理モジュール１２２によって、画像Ｉの事前選択されたピクセルの最下位ビットに埋め込まれる。

【００１７】

ブロック２０４において、画像認証モジュール１０８は、画像Ｉ１１０をランダム画像Ｘ＝$\mathrm{Shuffle}_{K}$（Ｉ）にシャッフルし、ここでシャッフリング関数$\mathrm{Shuffle}_{K}$（）はキーＫに依存する。この実現形態において、秘密キーに基づくシャッフリングが使用され、これは各ピクセルに対する近傍ピクセルを秘密にする。別の実現形態においては、ピクセルをランダムに入れ換える（ｐｅｒｍｕｔｅ）シャッフリング関数が使用されて、公的に開示される。これによって近傍ピクセル／サンプルがランダム化されて、その結果、通常の修正においては修正ピクセルが連結されているという事実を、改ざんされたピクセル位置同定モジュール１２０が利用して、改ざんされたピクセルと、ピクセルを弱い電子透かし処理するのに使用される、その近傍ピクセルとを区別することができる。改ざんされたピクセルの検出確率を上げるためにピクセルに弱い電子透かしを入れるために、通常、近傍ピクセルが使用されることを思い出されたい。ピクセルＰまたはその近傍ピクセルに対する修正は、ピクセルＰの完全性を乱し、弱い電子透かしによって検出することができる。画像Ｉと同じ大きさの２値ロゴＬを、画像認証モジュール１０８が使用して、弱い電子透かしの完全性を検査する。２値ロゴＬは、ユーザによって生成または選択される２値画像であり、改ざんされたピクセルを検出するために弱い電子透かし処理に広く使用されている。この実現形態においては、画像１１０だけがシャッフリング動作を受けるのに対して、ロゴＬはそれを受けない。代替的な一実現形態においては、ロゴＬは、画像Ｉと同じブロック２０４の動作を受ける、すなわちサンプルシャッフリング関数がロゴＬに適用される。

【００１８】
ブロック２０６において、Ｘ（シャッフリングされた画像）とロゴＬの両方が、ジグザグスキャン、行方向スキャン、または任意スキャンによって長さＮの１次元（１Ｄ）ベクトルに並べられ、ここでＮは画像Ｉ１１０におけるピクセル数である。説明を簡単にするために、これらの１Ｄベクトルは、なお各々ＸおよびＬによって表わすことにする。ここで留意すべきことは、２Ｄ画像と対応する１Ｄベクトルとの間には１対１の対応があることである。文脈においてどちらを使用するべきかを区別するのは容易であるので、このことから混乱を生じることはない。例えば、Ｘ（ｉ）などの単一指数のＸは、１ＤベクトルＸにおけるｉ番目の要素を意味するのに対して、Ｘ（ｉ，ｊ）などの２指数のＸは、２Ｄ画像Ｘのｉ番目の行とｊ番目の列にある要素を意味する。

【００１９】
ブロック２０８において、画像認証モジュール１０８は、Ｘ（変換画像）における全ピクセルを、第１および第２の分離された部分空間（ｄｉｓｊｏｉｎｔ　ｓｕｂｓｐａｃｅ）－ＡおよびＢ－を分割して、Ｂが末尾のｒピクセルを含み、Ａが残りのピクセルを含むようにする。Ｂにおける各ピクセルの最下位ビット（ＬＳＢ）はゼロに設定される。ｒの値については、ハッシュ動作に関係して以下で考察する。ブロック２１０において、画像認証モジュール１０８は、第１および第２の分離された部分空間の特定の部分空間において、ある関係を適用する。例えば、一実現形態においては、画像認証モジュール１０８は、分割Ｂの最下位ビットをすべてゼロにする。より具体的には、ｉ番目のピクセルＸ（ｉ）、ここでｉは１からＮまで変化する、に対して、画像認証モジュール１０８は、Ｘ（ｉ）を必要ならば入れ換えて、以下の関係：

【００２０】
【数１】

$$L(i) = f(X(i-1) \oplus X(i)), \quad 1 \le i \le N, \qquad \text{式 (1)}$$

【００２１】
を適用し、ここでＸ（０）＝０であり、

【００２２】
【数２】

$\oplus$

【００２３】
はＸＯＲ演算を表わす。Ｘ（ｉ）がＢに入る場合には、パータベーション（ｐｅｒｔｕｒｂａｔｉｏｎ）を加えた値は偶数、すなわち、パータベーション後のＬＳＢはまだ０である。この演算は、Ｘのすべてのピクセルに適用される。この実現形態では、マッピング式（１）において、先に電子透かし処理された１つのピクセルが使用される。別の実現形態においては、先に電子透かし処理された複数のピクセルが、マッピング式に使用される。

【００２４】
ブロック２１２において、画像認証モジュール１０８は、特定の部分空間Ｂの指定のビット部分に、ディジタル署名を埋め込む。例えば、一実現形態においては、画像認証モジュール１０８は、結果として得られるＸ（ブロック２０８からの結果）を、一方向暗号ハッシュ関数（ｏｎｅ－ｗａｙ　ｃｒｙｐｔｏｇｒａｐｈｉｃ　ｈａｓｈ　ｆｕｎｃｔｉｏｎ）Ｈ（例えば、ＳＨＡ１またはＭＤ５）を用いて、ハッシングする。一方向ハッシュ関数Ｈは、１Ｄベクトルなどの任意の列を、固定桁の列に変換する。一実現形態においては、画像認証モジュール２１２は、そのハッシュ値を、非対称暗号化の秘密鍵で暗号化して、ディジタル署名Ｄを生成する。分割化動作（ブロック２０８）におけるｒの値は、ビット数で表わしたＤの大きさである。Ｄは、Ｂにおけるピクセルの ＬＳＢに埋め込まれている。追加のデータを画像Ｉに埋め込む必要がある場合には、ｒの値は、Ｄおよび追加の情報の両方をビットで表わすのに十分なほど、大きくしなくてはならず、追加のデータはＤと一緒に埋め込まれる。

【００２５】
ブロック２１２の動作の別の実現形態においては、キー付のハッシュまたはＭＡＣが、ブロック２０８の動作の後に結果として得られるＸに適用されて、ダイジェスト（ｄｉｇｅｓｔ）Ｄが生成される。説明を簡単にするために、この値は、本稿においてはなおディジタル署名と呼ぶ。ハッシュ関数およびＭＡＣの使用は、ＭＡＣまたはキー付きハッシュが使用される場合には、それらは暗号化することなく、直接埋め込まれる点が異なっている。
【００２６】
ブロック２１４において、画像認証モジュール１０８は、ブロック２０６およびブロック２０４のスキャン動作およびシャッフリング動作を逆転させて、画像１１０に署名をするプロセスを終了する。
【００２７】
（例示的真正性検証）
図３は、画像認証のための例示的手順３００を示す。考察の目的で、この手順の観点を、図１の機能について考察する。構成要素参照番号の左端桁は、その構成要素が最初に現れる特定の図を識別する。信号真正性検証１１８は、障害のある画像Ｉ’（すなわち画像１１０）の真正性を次のように検証する。ブロック３０２において、障害のある画像１１０が入力される。障害のある画像は、署名がされており、かつ／またはその他の動作（既知および／または未知の動作）を受けている可能性がある。ブロック３０４において、シャッフリング関数$Shuffle_K$（）および秘密キーＫが、画像Ｉ’をシャッフルするのに使用されて、Ｘ’＝$Shuffle_K$（Ｉ’）を得る。このシャッフリング関数およびキーＫは、ブロック２０４において画像に署名するのに使用されたのと同じものである。このブロックにおける動作は、図２のブロック２０４における動作と同じである。ブロック３０６において、Ｘ’は、ブロック２０６で画像に署名するのに使用されたのと同じスキャン順序を使用して、長さの１Ｄベクトルに並べられ、ここでＮは障害のある画像Ｉ’におけるピクセル数である。ここでも、同じ記号Ｘ’を使用して、以下の説明において混乱することなく、２Ｄ画像Ｘ’およびそれの対応する１Ｄベクトルの両方を表わしている。
【００２８】
ブロック３０８において、Ｘ’における全ピクセルは、２つの分離された部分空間Ａ’およびＢ’に分割され、ここでＢ’は末尾のｒピクセルを含み、Ａ’は残りのピクセルを含む。一実現形態において、秘密キーＫ（ならびに実現形態によっては暗号解読のための公開キー）が、障害のある画像の検証のために使用される。上述の署名手順に対する代替的実現形態として記述されるように、Ｋが画像に埋め込まれている場合には、各署名画像１１０に対する秘密キーＫの複雑な管理は必要がない。ブロック３１０において、埋め込まれたＤ’は、部分空間Ｂ’におけるピクセルのＬＳＢから抽出される。ブロック３１２において、抽出されたＤ’は、公開キーを用いて暗号解読され、埋め込まれたハッシュ値ｈが回復される。このステップは、キー付きハッシュまたはＭＡＣを使用する場合には、必要ではない。ブロック３１４において、Ｂ’における各ピクセルの最下位ビット（ＬＳＢ）はゼロに設定される。ブロック３１６において、ハッシュ関数Ｈが、ブロック３１４からの結果に適用されて、障害のある画像Ｉ’のハッシュ値ｈ’、ｈ＝Ｈ（Ｘ’）を生成し、ここでＸ’はブロック３１４からの結果である。このハッシュ関数は、上述の署名手順と同じである。キー付きハッシュまたはＭＡＣが署名手順に使用される場合には、ブロック３１６において、同じ関数がブロック３１４からの結果に対して使用され、障害のある画像Ｉ’に対するｈ’が生成される。
【００２９】
ブロック３１８において、抽出されたハッシュ値ｈと新規に取得されたハッシュ値ｈ’とが一致するかどうかが決定される。ｈ＝ｈ’の場合には、手順３００の動作は、ブロック３２０へと続き、ここで障害のある画像Ｉ’が真正であることが指示される（真正指示１１２）。そうでない場合には、手順３００の動作は、ブロック３２２に続き、そこでＩ

’は真正でないと指示され（すなわち、真正でない画像Ｉ１１０は、１つまたは複数の改ざんされたピクセルを含む）、非真正指示１１２の結果となる。

【００３０】

（例示的改ざん位置同定）

図４は、改ざんされたピクセル位置同定の例示的手順４００を示す。考察の目的で、手順４００の観点を図１の特徴について考察する。構成要素参照番号の最左端ビットは、その構成要素が最初に現れる特定の図を識別する。真正でない画像Ｉ’１１０に対して、改ざんされたピクセル位置同定１２０は、次のように改ざんされたピクセルを位置同定（すなわち、識別）する。ブロック４０２において、シャッフリング関数$Shuffle_K$（）は、入力秘密キーを使用して、入力画像Ｉ’をシャッフルして、Ｘ’＝$Shuffle_K$（Ｉ’）を取得する。シャッフリング関数およびキーＫは、画像の署名に使用されたのと同じものである。

【００３１】

ブロック４０４において、Ｘ’は、署名手順の場合と同じスキャン順序で、長さＮの１Ｄベクトルに並べられ、ここでＮは障害のある画像Ｉ’におけるピクセル数である。先の説明と同様に、以下では、同じシンボルＸ’を使用して、混乱することなく、２Ｄ画像Ｘ’とそれに対応する１Ｄベクトルの両方を表わす。ブロック４０６において、Ｘ’におけるすべてのピクセルは、分離された部分空間Ａ’およびＢ’に分割され、ここでＢ’は末尾のｒピクセルを含み、Ａ’は残りのピクセルを含む。ブロック４０８において、部分空間Ｂ’における各ピクセルの最下位ビット（ＬＳＢ）がゼロに設定される。ブロック４１０において、秘密キーＫと、バイナリマッピング関数ｆを生成する署名手順にブロック２０２において使用されたものと同じ動作とを使用して、バイナリマッピング関数ｆが再生成される。このマッピングを使用してブロック４１２の結果が得られる。ブロック４１２において、式（１）がブロック４０８の結果に適用される。ブロック４１２からの結果を、抽出Ｌ’として参照する。ブロック４１４において、ブロック４０４の画像に適用するのと同じスキャン順序を使用して、原ロゴＬがスキャンされて１Ｄベクトルになる。この１Ｄベクトルはまだ Ｌで表わされる。ブロック４１６において、ロゴＬは２値画像であるので、不一致の画像ビット、すなわちピクセルを比較してマーキングすることによって、集合S_D＝｛ｉ｜Ｌ’（ｉ）≠Ｌ（ｉ）｝が識別される。ブロック４１８において、S_Dが拡張されて$S = S_D \cup \{i-1 \mid i \in S_D\}$が得られる。ブロック４２０において、Ｓが空であるかどうかが決定される。Ｓが空の場合には、改ざんされたピクセルは、このスキームによって位置同定することはできず、手順４００は終了する。Ｓが空でない場合には、手順はブロック４２２に続き、ここで１Ｄシーケンスが２Ｄ画像に変換される。この動作には、ブロック４０４において２Ｄ画像を１Ｄベクトルに変換するのに使用されたのと同じスキャン順序が使用される。この変換は、ブロック４０４の変換の逆動作である。この逆動作を実現する簡単な方法は、１Ｄベクトル内の各値を、２Ｄ画像内の対応するピクセルにコピーすることである。ブロック４２４において、ブロック４０２のシャッフリング動作は、逆転されて集合Ｓに対応するピクセルS^*の集合が位置同定される。例えば、ピクセル（ｉ，ｊ）が、シャッフリング動作において別のピクセル（ｍ，ｎ）に入れ換えられている場合には、ブロック４２４は、単にピクセル（ｍ，ｎ）を位置（ｉ，ｊ）に戻すことによって、シャッフリング動作を逆にする。S^*内のピクセルは、改ざんされている可能性がある。ブロック４２６において、絞り込み（ｒｅｆｉｎｅｍｅｎｔ）動作を使用してS^*におけるピクセルが絞り込まれる。例示的絞り込み動作について、以下の段落［００３２］から説明する。ブロック４２８において、真正でない画像Ｉ１１０の位置同定された改ざんされたピクセル１１４が出力される。

【００３２】

（安全性分析）

上述の実現形態においては、暗号ハッシュまたはＭＡＣ関数を使用して、ダイジェストまたはその暗号化バージョンを埋め込むのに使用される画像１１０ピクセルのＬＳＢを除き、画像１１０に対するディジタル署名が生成される（段落［００２３］のブロック２１

２の説明を参照）。暗号化ハッシュ関数またはＭＡＣ関数のあり得ない衝突（ｃｏｌｌｉｓｉｏｎ）が発生するときを除いて、署名された画像に対するいかなる変更も、真正性検証手順によって検出される。したがって、攻撃者が、オラクル攻撃または署名画像１１０に対するその他の知られている攻撃に成功することは不可能である。一方で、構成要素１２０の改ざん位置同定動作によって、一部の改ざんされたピクセルが検出できない可能性がある。説明した実現形態では、Ｙ－Ｍスキームにおける５０％の検出確率に比較して、$1-0.5^2=75\%$の確率で改ざんされたピクセルが位置同定される。改ざん位置同定能力の低下を犠牲にして、式（１）に使用される近傍ピクセルの数を増大させることによって、より高い検出確率を達成することができる。

【００３３】

より具体的には、一実現形態において、改ざん位置同定動作は、ピクセル近傍依存度基準によってさらに改善される。この実現形態は、実際の応用における典型的な動作によって画像１１０中に連結された修正ピクセルが得られるという事実を利用する。隔離されているか、またはその接続経路が事前設定閾値よりも小さい、Ｓ＊におけるピクセルが、Ｓ＊から除去される。Ｓ＊におけるピクセルＰの接続経路（ｃｏｎｎｅｃｔｅｄ　ｐａｔｈ）とは、Ｓ＊内の近傍ピクセルを通過してピクセルＰに達することのできる、Ｓ＊内のピクセルの数である。ここでの近傍の定義は、画像内の自然近傍であり、それは、本稿の別の場所で使用する、マッピング機能式（１）においてより多くのピクセルを導入するための近傍とは異なる。Ｓ＊における残りのピクセルは、改ざんされたピクセルとして識別される。この実現形態の改ざん位置同定の解像度は、実際の用途における典型的な画像データ操作に対して、Ｙ－Ｍスキームの結果と非常に近いながら、画像に署名する際に近傍として選択されるランダムピクセルによって、またピクセル近傍依存性基準の使用によって、改ざんされたピクセルの検出確率はより高いように思われる。言い換えると、記述した実現形態は、Ｙ－Ｍが可能なように、しかし、近傍依存性を使用するその他のスキームにおける一般的な拡張（ｅｘｐａｎｄｉｎｇ）なしに、単一ピクセルの精細さで改ざんされたピクセルを位置同定することができる。近傍依存性を使用するそれら他のスキームは、あるピクセルが実際に修正されているかどうか、またはその近傍ピクセルが実際に修正されているかどうかを簡単には判別できない。

【００３４】

図２の動作２１２においてキー付きハッシュまたはＭＡＣが使用される場合で、かつ、ｈおよびｈ’がブロック４１６において比較されるときに、不一致のビット数が、ハッシュビットの半分よりもずっと小さい場合には、不一致のビットに対応する、部分空間Ｂ’におけるピクセルのＬＳＢは、変更／操作されていると決定される。図２の動作２１２において、非対称暗号化が使用されるときには、そのような結論をすることはできない。埋め込むべきビット数もまた増加する。その利点は、認可された検定者、すなわち真正性検証および離散的改ざん位置同定を実行するために秘密にアクセスできるユーザまたはマシンは、偽造には秘密鍵が必要であるために、ディジタル署名を偽造することはできないことである。

【００３５】

（例示的動作環境）

必須ではないが、離散的改ざん位置同定による安全画像認証のためのシステムおよび方法を、パーソナルコンピュータなどのコンピュータ装置によって実行されるコンピュータ実行可能命令（プログラムモジュール）の一般的文脈で説明する。プログラムモジュールは、一般に、特定のタスクを実行するか、または特定の抽象データタイプを実装する、ルーチン類、プログラム類、オブジェクト、構成要素、データ構造、その他を含む。システムおよび方法を前述の文脈で説明したが、以下に説明する行為および動作はハードウエアで実現することもできる。

【００３６】

図５は、離散的改ざん位置同定による安全画像認証を完全にまたは部分的に実現できる、適当なコンピュータ環境の例を示している。例示的コンピュータ環境５００は、図１の

例示的システムおよび図２から図４の例示的動作のための適当なコンピュータ環境の一例にすぎず、本明細書に記述するシステムおよび方法の使用または機能の範囲についての限定を示唆するものではない。またコンピュータ環境５００も、コンピュータ環境５００に示す構成要素の任意のもの、またはその組合せに関係する、依存性または要件を有するとは解釈すべきではない。

【００３７】

本明細書に記載する方法およびシステムは、その他多数の汎用または専用のコンピュータシステム、環境または構成において動作可能である。使用に適する周知のコンピュータシステム、環境、および／または構成の例としては、それに限定はされないが、パーソナルコンピュータ、サーバコンピュータ、マルチプロセッサシステム、マイクロプロセッサベースシステム、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ、前述のシステムまたは装置の任意のものを含む分散コンピューティング環境、その他が挙げられる。これらのフレームワークのコンパクトバージョンまたはサブセットバージョンも、ハンドヘルドコンピュータなどの限られた資源のクライアント、またはその他のコンピュータ装置に実装することができる。本発明は、通信ネットワークを介して連結されるリモート処理装置によってタスクが実行される、分散コンピューティング環境において実施される。分散コンピュータ環境においては、プログラムモジュールは、ローカル記憶装置およびリモート記憶装置の両方に配置することができる。

【００３８】

図５を参照すると、離散的改ざん位置同定による安全画像認証の例示的システムは、例えば、図１のシステム１００を実装するコンピュータ５１０の形態の、汎用コンピュータ装置を含む。以下に記述するコンピュータ５１０の観点は、図１のクライアントコンピュータ装置１０２の例示的実現形態である。コンピュータ５１０の構成要素としては、それに限定はされないが、処理ユニット５２０、システムメモリ５３０、およびシステムメモリを含み様々なシステム構成要素を処理ユニット５２０に結合する、システムバス５２１を含めることができる。システムバス５２１は、メモリバスまたはメモリコントローラ、周辺バス、および様々なバスアーキテクチャの任意のものを使用するローカルバスを含む、いくつかの種類のバス構造のいずれかとすることができる。限定ではなく一例として、そのようなアーキテクチャとしては、ＩＳＡ（Ｉｎｄｕｓｔｒｉａｌ　Ｓｔａｎｄａｒｄ　Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＭＣＡ（Ｍｉｃｒｏ　Ｃｈａｎｎｅｌ　Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＥＩＳＡ（Ｅｎｈａｎｃｅｄ　ＩＳＡ）バス、ＶＥＳＡ（Ｖｉｄｅｏ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｓｔａｎｄａｒｄｓ　Ａｓｓｏｃｉａｔｉｏｎ）ローカルバス、およびＭｅｚｚａｎｉｎｅバスと呼ばれるＰＣＩ（Ｐｅｒｉｐｈｅｒａｌ　Ｃｏｍｐｏｎｅｎｔ　Ｉｎｔｅｒｃｏｎｎｅｃｔ）バスが挙げられる。

【００３９】

コンピュータ５１０は、通常、様々なコンピュータ読取可能な媒体を含む。コンピュータ読取可能な媒体は、コンピュータ５１０によってアクセスすることのできる任意の利用可能な媒体を含むとともに、揮発性および不揮発性の媒体、取外し可能および固定の媒体の両方が挙げられる。限定としてではなく一例として、コンピュータ読取可能な媒体には、コンピュータ記憶媒体および通信媒体を含めることができる。コンピュータ記憶媒体としては、コンピュータ読取可能な命令、データ構造、プログラムモジュールまたはその他などの情報の記憶のための、任意の方法または技術によって実現される、揮発性および不揮発性、取外し可能および固定の媒体が挙げられる。コンピュータ記憶媒体としては、それに限定はされないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリまたはその他のメモリテクノロジ、ＣＤ－ＲＯＭ、ＤＶＤまたはその他の光ディスク記憶、磁気カセット、磁気テープ、磁気ディスク記憶またはその他の磁気記憶装置、または所望の情報を記憶することができ、かつコンピュータ５１０によってアクセスすることのできる、その他任意の媒体が挙げられる。

【００４０】

通信媒体には、通常、コンピュータ読取可能な命令、データ構造、プログラムモジュー

ル、または搬送波またはその他の移送機構などの変調データ信号としてのその他のデータが組み入れられるとともに、任意の情報配信媒体を含む。「変調データ信号」の用語は、１つまたは複数の特徴セットを有するか、または信号中に情報を符号化するように変化させた信号を意味する。限定ではなく一例として、通信媒体としては、有線ネットワークまたは直接有線接続などの有線媒体、ならびに音響、ＲＦ、赤外線およびその他の無線媒体が挙げられる。前記の任意のものの組合せも、コンピュータ読取可能な媒体の範囲に含めるべきである。

【００４１】

システムメモリ５３０は、読取り専用メモリ（ＲＯＭ）５３１やランダムアクセスメモリ（ＲＡＭ）５３２などの揮発性メモリおよび／または不揮発性メモリの形態のコンピュータ記憶媒体を含む。起動時などにコンピュータ５１０内部の要素間の情報の転送を助ける基本ルーチンを含む、基本入出力システム５３３（ＢＩＯＳ）は、通常、ＲＯＭ５３１内に記憶されている。ＲＡＭ５３２は、通常、処理ユニット５２０に直接アクセス可能で、かつ／または現在それによって実行されている、データおよび／またはプログラムモジュールを収容する。限定ではなく一例として、図５はオペレーティングシステム５３４、アプリケーションプログラム５３５、その他のプログラムモジュール５３６、およびプログラムデータ５３８を示す。

【００４２】

コンピュータ５１０には、その他の取外し可能／固定の、揮発性／不揮発性コンピュータ記憶媒体を含めることができる。一例としてだけであるが、図５は、取り出し不能、不揮発性磁気媒体の読取りまたは書込みを行うハードディスクドライブ５４１、取外し可能な不揮発性磁気ディスク５５２の読取りまたは書込みを行う磁気ディスクドライブ５５１、およびＣＤＲＯＭまたはその他の光媒体などの取外し可能な不揮発性光ディスク５５６の読取りまたは書込みを行う光ディスクドライブ５５５を示している。この例示的オペレーティング環境において使用できるその他の取外し可能／固定の、揮発性／不揮発性コンピュータ記憶媒体としては、それに限定はされないが、磁気テープカセット、フラッシュメモリカード、ＤＶＤ、ディジタルビデオテープ、ソリッドステートＲＡＭ、ソリッドステートＲＯＭ、その他が挙げられる。ハードディスクドライブ５４１は、通常、インターフェイス５４０などの固定のメモリインターフェイスを介してシステムバス５２１に接続され、磁気ディスクドライブ５５１および光ディスク５５５は、通常、インターフェイス５５０などの、取外し可能なメモリインターフェイスによってシステムバス５２１に接続される。

【００４３】

上記して図５に示したドライブ類およびそれらに付随するコンピュータ記憶媒体は、コンピュータ５１０のコンピュータ読取可能な命令、データ構造、プログラムモジュールおよびその他のデータの記憶装置を提供する。図５においては、例えば、ハードディスクドライブ５４１は、オペレーティングシステム５４４、アプリケーションプログラム５４５、その他のプログラムモジュール５４６、およびプログラムデータ５４８を記憶する状態で示してある。ここで留意すべきことは、これらの構成要素は、オペレーティングシステム５３４、アプリケーションプログラム５３５、その他のプログラムモジュール５３６、およびプログラムデータ５３８と同じであっても、異なっていてもよいことである。アプリケーションプログラム５３５は、例えば、図１のプログラムモジュール１０４を含む。プログラムデータ５３８は、例えば、図１のプログラムデータ１０６を含む。オペレーティングシステム５４４、アプリケーションプログラム５４５、その他のプログラムモジュール５４６、およびプログラムデータ５４８は、それらは少なくとも異なるコピーであることを示すために、異なる数字を与えてある。

【００４４】

ユーザは、一般にマウス、トラックボールまたはタッチパッドと呼ばれる、キーボード５６２およびポインティング装置５６１などの入力装置を介してコンピュータ５１０にコマンドおよび情報を入力することができる。その他の入力装置（図示せず）としては、マ

イクロフォン、ジョイスティック、ゲームパッド、サテライトディッシュ、スキャナー、その他が挙げられる。これらおよびその他の入力装置は、システムバス５２１に結合されたユーザ入力インターフェイス５６０を介して処理ユニット５２０に接続されることが多いが、パラレルポート、ゲームポートまたはＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）などの、その他のインターフェイスまたはバス構造によって接続することもできる。

【００４５】

モニター５９１またはその他の種類のディスプレイ装置を、ビデオインターフェイス５９０などのインターフェイスを介してシステムバス５２１に接続することもできる。モニターに加えて、コンピュータには、スピーカ５９８やプリンタ５９６などの、その他の周辺出力装置を含めて、これらは出力周辺インターフェイス５９５を介して接続することもできる。

【００４６】

コンピュータ５１０は、リモートコンピュータ５８０などの、１つまたは複数のリモートコンピュータへの論理接続を使用するネットワーク環境内で動作する。リモートコンピュータ５８０は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイスまたはその他の共通ネットワークノードとしてもよく、またその特定の実現形態の機能として、図５にはメモリ記憶装置５８１だけを示してあるが、コンピュータ５１０に関して上述した多く、または全部の要素を含めてもよい。図５に示す論理接続は、ローカルエリアネットワーク（ＬＡＮ）５８１およびワイドエリアネットワーク（ＷＡＮ）５８３を含むが、その他のネットワークを含めてもよい。そのようなネットワーク環境は、事務所、企業内コンピュータネットワーク、イントラネットおよびインターネットにおいて普及している。

【００４７】

ＬＡＮネットワーク環境において使用されるときに、コンピュータ５１０は、ネットワークインターフェイスまたはアダプタ５８０を介してＬＡＮ５８１に接続される。ＷＡＮネットワーク環境において使用されるときには、コンピュータ５１０は、通常、インターネットなどのＷＡＮ５８３上での通信を確立するためのモデム５８２またはその他の手段を含む。モデム５８２は、内部式でも外部式でもよく、ユーザ入力インターフェイス５６０、またはその他の適当な機構を介してシステムバス５２１に接続することができる。ネットワーク環境においては、コンピュータ５１０またはその部分に対して示したプログラムモジュールは、リモート記憶装置に記憶することができる。限定ではなく一例として、図５はメモリ装置５８１に常駐するリモートアプリケーションプログラム５８５を示す。図示したネットワーク接続は、例示的なものであり、コンピュータ間の通信リンクを確立するその他の手段を使用することができる。

【００４８】

（結論）

離散的改ざん位置同定による安全画像認証のためのシステムおよび方法を、構造特徴および／または方法論的選択肢または作用に特有の言語で説明したが、添付のクレイムに定義された実現形態は、必ずしも記述した特定の特徴または作用に限定されるものではない。例えば、このシステムおよび方法は、グレースケール画像について記述したが、このシステムおよび方法は、当業者によってカラー画像、音声およびビデオデータに対して容易に実装して実現することができる。したがって、具体的な特徴および動作は、請求される主題の例示的形態として開示されるものである。

【図面の簡単な説明】

【００４９】

【図１】離散的改ざん位置同定による安全画像認証のための例示的システムを示す図である。

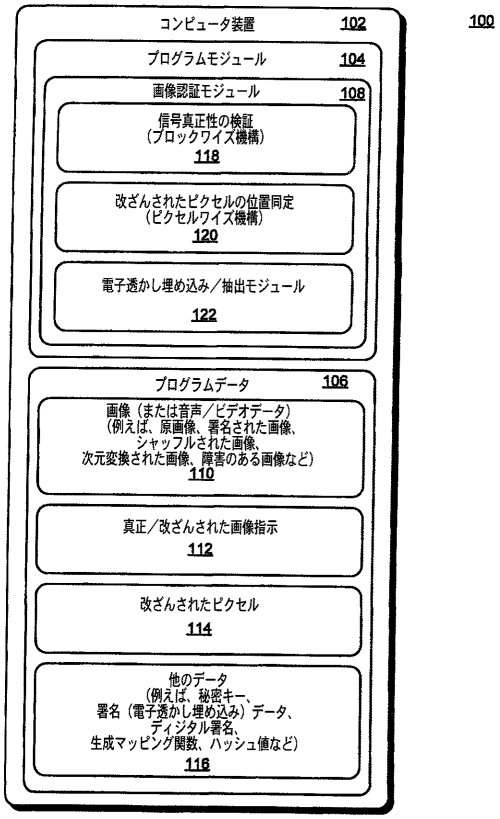
【図２】画像などのマルチメディアに署名をするための例示的手順を示す図である。

【図３】図１のシステムにおける安全画像認証のための例示的手順を示す図である。

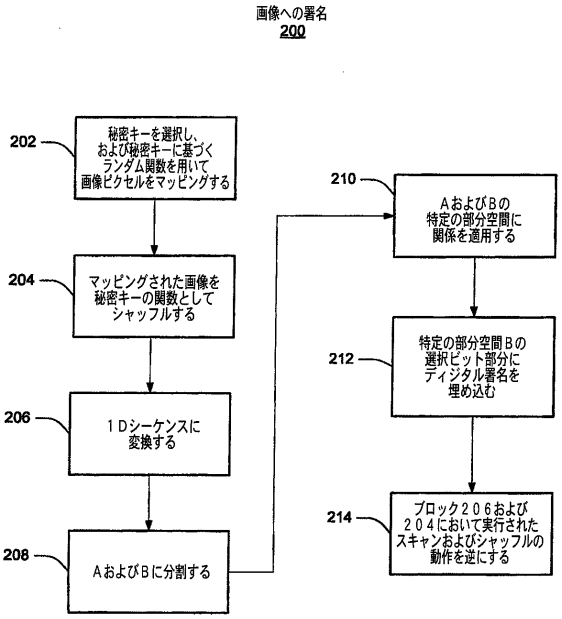
【図４】図１のシステムにおける改ざんされたピクセル位置同定の例示的手順を示す図である。

【図５】離散的改ざん位置同定による安全画像認証を完全または部分的に実装することのできる、適当なコンピュータ環境の例を示す図である。

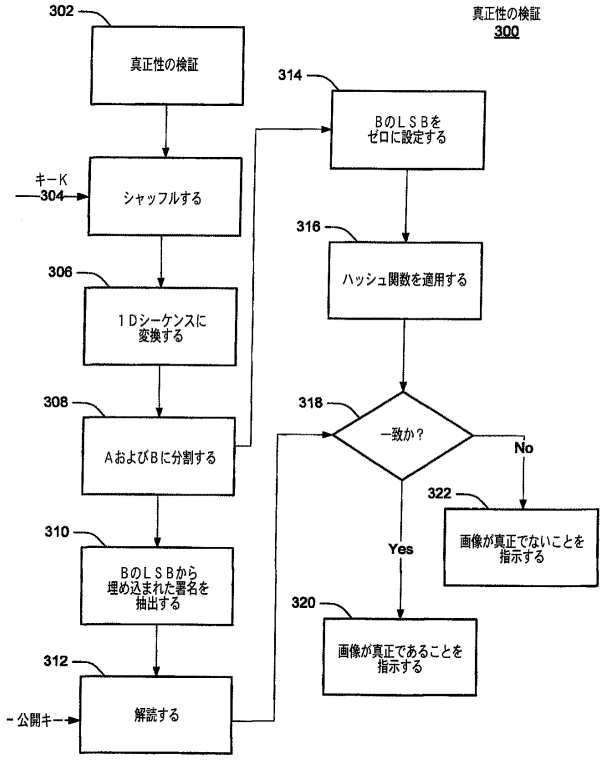
【図１】



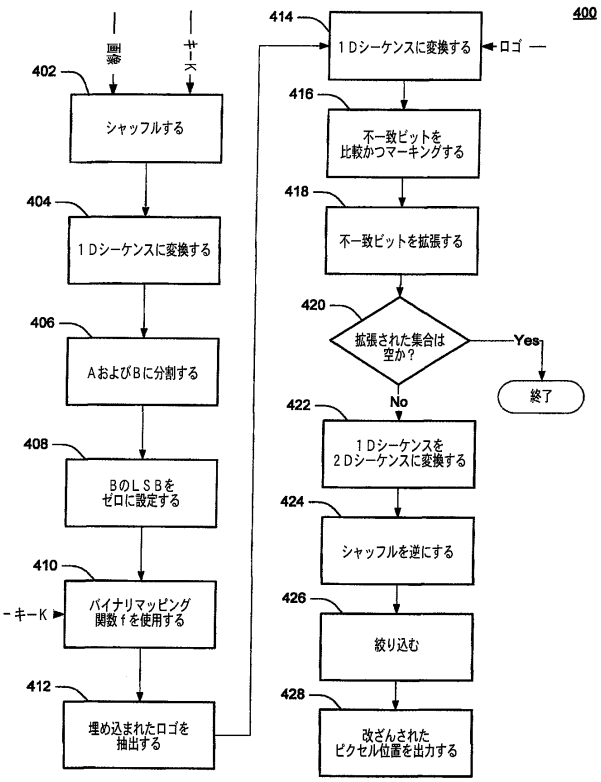
【図２】



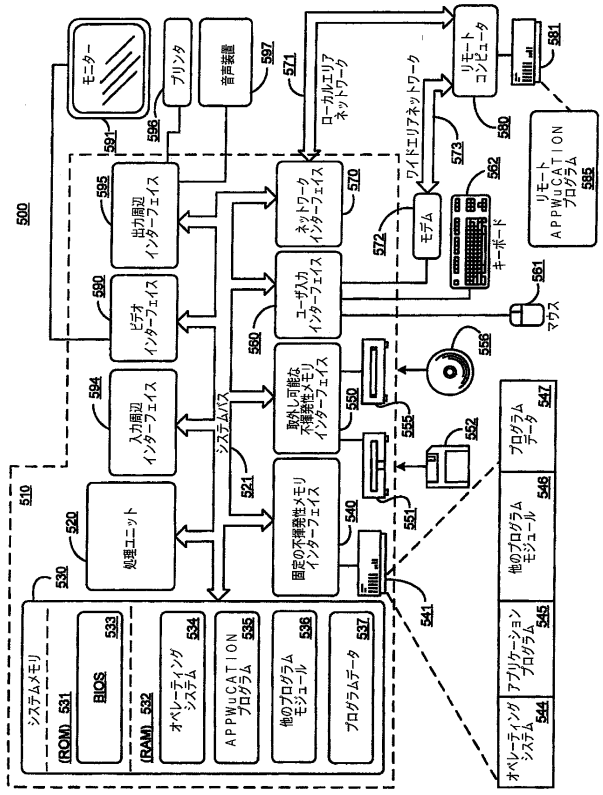
【図３】


真正性の検証
300
302
真正性の検証
キーK
304
シャッフルする
306
１Ｄシーケンスに変換する
308
ＡおよびＢに分割する
310
ＢのＬＳＢから埋め込まれた署名を抽出する
312
解読する
公開キー
314
ＢのＬＳＢをゼロに設定する
316
ハッシュ関数を適用する
318
一致か？
No
Yes
320
画像が真正であることを指示する
322
画像が真正でないことを指示する

【図４】


400
画像
キー
402
シャッフルする
404
１Ｄシーケンスに変換する
406
ＡおよびＢに分割する
408
ＢのＬＳＢをゼロに設定する
410
バイナリマッピング関数ｆを使用する
キーK
412
埋め込まれたロゴを抽出する
414
１Ｄシーケンスに変換する
ロゴ
416
不一致ビットを比較かつマーキングする
418
不一致ビットを拡張する
420
拡張された集合は空か？
Yes
終了
No
422
１Ｄシーケンスを２Ｄシーケンスに変換する
424
シャッフルを逆にする
426
絞り込む
428
改ざんされたピクセル位置を出力する

【図５】


500
510
520
530
処理ユニット
システムメモリ
(ROM) 531
BIOS 533
(RAM) 532
オペレーティングシステム 534
APPWuCATION プログラム 535
他のプログラムモジュール 536
プログラムデータ 537
システムバス 521
固定の不揮発性メモリインターフェイス 540
取外し可能な不揮発性メモリインターフェイス 550
入力周辺インターフェイス 594
ビデオインターフェイス 590
出力周辺インターフェイス 595
ユーザ入力インターフェイス 560
ネットワークインターフェイス 570
ローカルエリアネットワーク 571
ワイドエリアネットワーク 573
モデム 572
キーボード 562
マウス 561
リモートコンピュータ 580
リモート APPWuCATION プログラム 585
モニター 591
プリンタ 596
音声装置 597
プログラムデータ 547
他のプログラムモジュール 546
アプリケーションプログラム 545
オペレーティングシステム 544

フロントページの続き

(72)発明者　チンハイ　ウー
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　シャイペン　リー
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

審査官　白石　圭吾

(56)参考文献　特開２００１－０２４８７６（ＪＰ，Ａ）
特開２０００－１５５８３４（ＪＰ，Ａ）
特開２００１－０３６８５６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｎ　　１／３８７