

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-344718
(P2002-344718A)

(43) 公開日 平成14年11月29日 (2002. 11. 29)

(51) Int.Cl. ⁷	識別記号	F I	テ-マコード [*] (参考)
H 0 4 N 1/387		H 0 4 N 1/387	5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 A 5 C 0 7 6
	1 4 0	17/60	1 4 0 5 J 1 0 4
	1 4 2		1 4 2
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 D
審査請求 有 請求項の数15 OL (全 13 頁)			

(21) 出願番号 特願2001-143513(P2001-143513)

(22) 出願日 平成13年5月14日 (2001. 5. 14)

(71) 出願人 391016923

北海道大学長

北海道札幌市北区北8条西5丁目8番地

(72) 発明者 長谷山 美紀

北海道札幌市北区北6条西6丁目2-1-503

(74) 代理人 100072051

弁理士 杉村 興作 (外1名)

Fターム(参考) 5B017 AA03 BA09 CA16

5C076 AA14 BA06

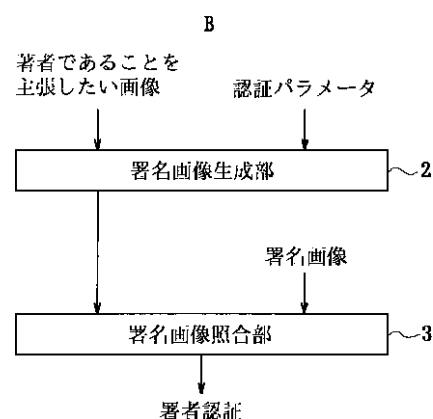
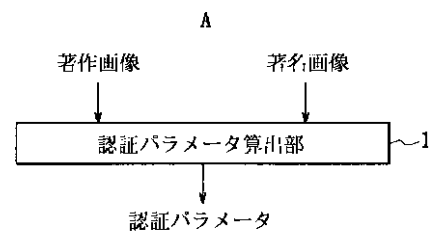
5J104 AA07 AA15 AA41 KA01 PA07

(54) 【発明の名称】 著者認証システム及び方法並びにコンピュータによって実行されるプログラム

(57) 【要約】

【課題】 提供されるデータの品質を下げることなく著者の認証を行う。

【解決手段】 認証パラメータ算出部1は、著作画像及び署名画像から、著作画像の特徴を表現する認証パラメータを算出する。署名画像生成部2は、認証パラメータと、著者であることを主張したい画像とから、署名画像を生成する。署名画像照合部3は、署名画像生成部2によって生成された署名画像と、認証パラメータを算出する際に用いられた署名画像とを照合し、これらが同一である場合には著者の認証を行う。



【特許請求の範囲】

【請求項 1】 著者の作成した第 1 データ及び著者であることを証明する第 2 データから、前記第 1 データの特徴を表現する認証パラメータを算出する認証パラメータ算出手段と、

前記認証パラメータと、著者であることを主張したい第 3 データとから、前記第 2 データを生成する第 2 データ生成手段と、

前記第 2 データ生成手段によって生成された第 2 データと、前記認証パラメータを算出する際に用いられた第 2 データとを照合し、これらが同一である場合には前記第 3 データの著者を認証する第 2 データ照合手段とを具備することを特徴とする著者認証システム。

【請求項 2】 前記認証パラメータを I F S パラメータとしたことを特徴とする請求項 1 記載の著者認証システム。

【請求項 3】 前記第 2 データ生成手段による第 2 データの生成を、I F S に基づいて行ったことを特徴とする請求項 2 記載の著者認証システム。

【請求項 4】 前記認証パラメータを、フラクタル符号化によって算出したことを特徴とする請求項 1 から 3 のうちのいずれか 1 項に記載の著者認証システム。

【請求項 5】 前記第 1 - 3 データを、画像データ、文書データ又は音声データとしたことを特徴とする請求項 1 から 4 のうちのいずれか 1 項に記載の著者認証システム。

【請求項 6】 著者の作成した第 1 データ及び著者であることを証明する第 2 データから、前記第 1 データの特徴を表現する認証パラメータを算出する認証パラメータ算出ステップと、

前記認証パラメータと、著者であることを主張したい第 3 データとから、前記第 2 データを生成する第 2 データ生成ステップと、

前記第 2 データ生成ステップで生成された第 2 データと、前記認証パラメータを算出する際に用いられた第 2 データとを照合し、これらが同一である場合には前記第 3 データの著者を認証する第 2 データ照合ステップとを具備することを特徴とする著者認証方法。

【請求項 7】 前記認証パラメータを I F S パラメータとすることを特徴とする請求項 6 記載の著者認証方法。

【請求項 8】 前記第 2 データ生成ステップによる第 2 データの生成を、I F S に基づいて行うことを特徴とする請求項 7 記載の著者認証方法。

【請求項 9】 前記認証パラメータを、フラクタル符号化によって算出することを特徴とする請求項 6 から 8 のうちのいずれか 1 項に記載の著者認証方法。

【請求項 10】 前記第 1 - 3 データを、画像データ、文書データ又は音声データとすることを特徴とする請求項 6 から 9 のうちのいずれか 1 項に記載の著者認証方法。

【請求項 11】 著者の作成した第 1 データ及び著者であることを証明する第 2 データから、前記第 1 データの特徴を表現する認証パラメータを算出する認証パラメータ算出ステップと、

前記認証パラメータと、著者であることを主張したい第 3 データとから、前記第 2 データを生成する第 2 データ生成ステップと、

前記第 2 データ生成ステップで生成された第 2 データと、前記認証パラメータを算出する際に用いられた第 2 データとを照合し、これらが同一である場合には前記第 3 データの著者を認証する第 2 データ照合ステップとを具備することを特徴とするコンピュータによって実行される著者認証プログラム。

【請求項 12】 前記認証パラメータを I F S パラメータとすることを特徴とする請求項 11 記載のコンピュータによって実行される著者認証プログラム。

【請求項 13】 前記第 2 データ生成ステップによる第 2 データの生成を、I F S に基づいて行うことを特徴とする請求項 12 記載のコンピュータによる著者認証プログラム。

【請求項 14】 前記認証パラメータを、フラクタル符号化によって算出することを特徴とする請求項 11 から 13 のうちのいずれか 1 項に記載のコンピュータによる著者認証プログラム。

【請求項 15】 前記第 1 - 3 データを、画像データ、文書データ又は音声データとすることを特徴とする請求項 11 から 14 のうちのいずれか 1 項に記載のコンピュータによる著者認証プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネット産業やソフトウェア開発のようなデジタルコンテンツ配布に関わる電子工学における画像処理分野で利用される著者認証システム及び方法並びにコンピュータによって実行されるプログラムに関するものである。

【0002】

【従来の技術】近年、インターネットの普及に伴い、音楽や画像のようなデジタルコンテンツに触れる機会が増えている。また、様々なソフトウェアの開発によって、高い品質を保持した状態でデジタルコンテンツの編集や複製を、一般のユーザでも容易に行えるようになっている。

【0003】その結果、ネットワーク上のデジタルコンテンツは、不特定多数の利用者によってコピーされ、無断で利用され、さらにはネットワーク上での公開がなされるおそれがある。

【0004】これらの不正使用に対する対策として、デジタルコンテンツの著作権保護を目的として様々な電子透かしの研究が行われている。電子透かしは、埋め込みが行われる領域によって、空間領域利用型と周波数領域

利用型とに大まかに分類される。

【0005】

【発明が解決しようとする課題】空間利用型の電子透かしでは、一般に、埋め込まれた透かし情報がデータの圧縮、平滑化、拡大等によって消失しやすいという課題がある。一方、周波数領域利用型の電子透かしでは、透かし情報を周波数領域に埋め込むために、FFT、DCT等の直交変換によって、データを周波数に変換する。直交変換を施す各ブロックに透かし情報が埋め込まれるので、復号化された署名済みデータにブロック歪みが生じるおそれがある。また、いずれの型の電子透かしにおいても、著作データに透かし情報を埋め込むので、提供されるデータの品質低下を避けることができない。

【0006】本発明の目的は、提供されるデータの品質を下げることなく著者の認証を行うことができる著者認証システム及び方法並びにコンピュータによって実行されるプログラムを提供することである。

【0007】

【課題を解決するための手段】本発明による著者認証システムは、著者の作成した第1データ及び著者であることを証明する第2データから、前記第1データの特徴を表現する認証パラメータを算出する認証パラメータ算出手段と、前記認証パラメータと、著者であることを主張したい第3データとから、前記第2データを生成する第2データ生成手段と、前記第2データ生成手段によって生成された第2データと、前記認証パラメータを算出する際に用いられた第2データとを照合し、これらが同一である場合には前記第3データの著者を認証する第2データ照合手段とを具えることを特徴とする。

【0008】本発明によれば、従来行われているような著作データに署名を埋め込む手法とは異なり、第2データを生成するための第1データを保持するので、第3データすなわち著作データがそのままユーザに配布される。このように画像の構造を利用して第2データすなわち署名データを生成しているため、著作データに署名を埋め込む必要がなくなり、その結果、提供されるデータの品質を下げることなく著者の認証を行うことができるようになる。また、圧縮や平滑化に対する耐性が、従来行われているような著作画像に署名を埋め込む手法よりも高くなる。

【0009】なお、第2データ生成手段によって生成された第2データが劣化したとしても、認証パラメータを算出する際に用いられた第2データと認識される程度の劣化である場合には、これらの第2データは同一であると認められるものとする。

【0010】本発明による著者認証方法は、著者の作成した第1データ及び著者であることを証明する第2データから、前記第1データの特徴を表現する認証パラメータを算出する認証パラメータ算出ステップと、前記認証パラメータと、著者であることを主張したい第3データ

とから、前記第2データを生成する第2データ生成ステップと、前記第2データ生成ステップで生成された第2データと、前記認証パラメータを算出する際に用いられた第2データとを照合し、これらが同一である場合には前記第3データの著者を認証する第2データ照合ステップとを具えることを特徴とする。

【0011】本発明によれば、提供されるデータの品質を下げることなく著者の認証を行うことができるようになり、かつ、圧縮や平滑化に対する耐性が、従来行われているような著作画像に署名を埋め込む手法よりも高くなる。

【0012】本発明によるコンピュータによって実行される著者認証プログラムは、著者の作成した第1データ及び著者であることを証明する第2データから、前記第1データの特徴を表現する認証パラメータを算出する認証パラメータ算出ステップと、前記認証パラメータと、著者であることを主張したい第3データとから、前記第2データを生成する第2データ生成ステップと、前記第2データ生成ステップで生成された第2データと、前記認証パラメータを算出する際に用いられた第2データとを照合し、これらが同一である場合には前記第3データの著者を認証する第2データ照合ステップとを具えることを特徴とする。

【0013】本発明によれば、コンピュータによって、提供されるデータの品質を下げることなく著者の認証を行うことができるようになる。

【0014】前記認証パラメータを、例えばIFSパラメータとする。この場合、前記第2データ生成手段による第2データの生成を、IFSに基づいて行う。また、前記認証パラメータを、例えばフラクタル符号化によって算出する。

【0015】

【発明の実施の形態】本発明による著者認証システム及び方法並びにコンピュータによって実行されるプログラムの実施の形態を、図面を参照して詳細に説明する。図1は、本発明による著者認証システムを説明するための図である。本発明による著者認証システムでは、図1Aに示すような認証パラメータの算出と、図1Bに示すような画像の著者認証を行う。

【0016】認証パラメータ算出部1は、それに入力された著作画像及び署名画像（著者であることを証明する画像）から、著作画像の特徴を表現する認証パラメータを算出する。算出された認証パラメータは、図示しないメモリ（例えばEPROM）に保持される。なお、認証パラメータを、例えば、後に説明するようにIFS(Iterated Function System)パラメータとする。

【0017】署名画像生成部2は、図示しないメモリに保持された識別パラメータと、著者であることを主張したい画像とを用いて、署名画像を生成する。生成された署名画像は、署名画像照合部3に入力される。署名画像

照合部3では、署名画像生成部2で生成された署名画像と、認証パラメータを算出するのに用いた署名画像とを照合する。これらの署名画像が同一である場合には、著者の認証を行う。

【0018】署名画像が同一であるとは、一般に、署名画像を構成する全画素の濃淡値が同一であることを意味するが、署名画像としてシンボルや文字を採用した場合には、その同一性は、全画素の濃淡値が同一でなくても、同一シンボルや同一文字と認識される程度の劣化が生じたとしても同一であると認められる。

【0019】本実施の形態では、従来行われているような著作画像に署名を埋め込む手法とは異なり、署名を抽出するための認証パラメータを保持するので、著作画像がそのままユーザに配布される。このように画像の構造を利用して署名画像を生成しているため、圧縮や平滑化に対する耐性が、従来行われているような著作画像に署名を埋め込む手法よりも高くなる。なお、上記手順は、図示しないメモリ（例えばフラッシュメモリ）に格納されたプログラムを図示しないCPUが読み出すことによって実行される。

【0020】本実施の形態では、認証パラメータは、A. E. Jacquin: "Image coding based on fractal theory of iterated contractive image transformation", IEEE Trans. on Image Processing, 1, 1, pp. 18-30に記載されているようなフラクタル画像符号化に基づいて算出される。

【0021】認証パラメータの算出過程を、図2を用いて説明すると、まず、 $N \times M$ 画素の署名画像4を、互いに重なり合わない $B \times B$ 画素のブロック R_i ($i = 1, 2, \dots, n | n = N / B \times M / B$)に分割する。これらのブロックをレンジブロックとする。

【0022】次に、 $N \times M$ 画素の著作画像5を、 $2B \times 2B$ 画素のブロック D_j ($j = 1, 2, \dots, m | m = (N - 2B + 1)(M - 2B + 1)$)に分割する。これらのブロックをドメインブロックとする。

【0023】次に、各レンジブロック R_i ($i = 1, 2, \dots, n$)

$$z = z' \times s + o$$

の演算を施すことによって、レンジブロック R_i 内の画素に対する輝度値が算出される。

【0028】これらドメインブロックの決定及び輝度値の算出は、各レンジブロック R_i ($i = 1, 2, \dots, n$)について繰り返され、これによって、署名画像生成部2が署名画像を生成する。

【0029】なお、 z' は、各レンジブロック R_i に対する縮小ドメインブロック D_k' 内の画素に対する輝度値を表し、 z は、生成される署名画像内の画素に対する輝度値を表す。また、 s, o は、各レンジブロック R_i に対して算出された認証パラメータに含まれる輝度値変換パラメータである。

【0030】署名画像照合部3は、署名画像生成部2に

2, ..., n) に対して最良の近似を与えるドメインブロック D_k ($1 \leq k \leq m$)を求めるために、上記A.

E. Jacquin: "Image coding based on fractal theory of iterated contractive image transformation", IEEE Trans. on Image Processing, 1, 1, pp. 18-30に記載されているようなドメインブロック D_j のアフィン変換 w_{ij} を行うとともに、各レンジブロック R_i に対して平均二乗誤差(MSE)が最小となる縮小ドメインブロック D_j' を求め、得られたパラメータを認証パラメータとする。

【0024】なお、認証パラメータは、1個のレンジブロックに対して、ドメインブロックの位置情報、アフィン変換による回転・反転パラメータ、スケーリングパラメータ等が算出する。また、1画像($N \times M$ 画素)に対して、 $n (= N / B \times M / B)$ 個のレンジブロックが存在する。このようにして算出された認証パラメータは、署名認証システムにおいて署名画像を浮き出させる鍵となる。

【0025】ここで、署名画像生成部2及び署名画像照合部3の動作を詳細に説明する。なお、本実施の形態では、署名画像生成部2は、IFSに基づいて設計される。まず、 $N \times M$ 画素の入力画像と、認証パラメータ算出部1から取得した認証パラメータを用意する。

【0026】署名画像生成部2によって生成される署名画像のサイズを $N \times M$ とし、互いに重なり合わない $B \times B$ 画素のレンジブロック R_i ($i = 1, 2, \dots, n | n = N / B \times M / B$)に分割する。また、著者であることを主張したい画像を、 $2B \times 2B$ 画素のドメインブロック D_j ($j = 1, 2, \dots, m | m = (N - 2B + 1)(M - 2B + 1)$)に分割する。

【0027】次いで、認証パラメータを参照して、レンジブロック R_i 内の画素に対する輝度値を算出するために必要なドメインブロックを決定する。このドメインブロックに対して、上記アフィン変換を施すことによって、縮小ドメインブロック D_k' が定まる。さらに、この縮小ドメインブロック D_k' に、

$$(1)$$

よって生成した署名画像と、認証パラメータ算出部1に入力された署名画像とを照合し、これらが一致すれば、著作画像の著者と認定される。

【0031】ここで、IFSと本発明による著者認証システムとの相違点について説明する。IMFでは、画像の持つ自己相似性に着目し、画像の構造的な特徴を表すIFSパラメータを算出する。そのパラメータを繰り返し利用することによって画像を発生させる。なお、ここでいう繰り返しとは、署名画像生成部2で実行される手順を更に繰り返すことを意味する。すなわち、IFSに基づく画像の生成手順によって、生成された画像(レンジブロック領域)を新たなドメインブロック探索領域と再び定め、画像の生成手順を繰り返すことをいう。IFS

Sパラメータが画像の自己相似性に基づいて算出されているので、反復によって、生成される画像の精度が向上する。

【0032】しかしながら、本発明による著者認証システムでは、IFSとは異なり、署名画像の生成手順で繰り返しを行わない。本発明による著者認証システムでは、著作画像（ドメインブロック探索領域）に基づいて、認証パラメータを用いることによって署名画像（レンジブロック領域）が生成される。すなわち、著作画像の特徴に基づく認証パラメータを利用するので、認証システムにおけるドメインブロック探索領域は、著作画像でなければ署名が抽出されないからである。

【0033】ここで、本発明による著者認証システムにおける署名画像の照合及び著者の認証が適切に行われていることを示すために、本発明が以下の条件を満足することを示す。

(i) 著作画像及び認証パラメータと、それから抽出される署名画像との組合せは一つのみ存在し、同一の認証パラメータを著作画像以外の画像に適用した場合、同一の署名画像が抽出されることはない、すなわち、著作画像以外の画像から同一の署名画像が抽出されることはない。

(ii) 攻撃によって著作画像が劣化した程度と、それか

$$\begin{aligned} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} &= v_{ij} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \\ &= \begin{pmatrix} \cos \theta & \mp \sin \theta & 0 \\ \sin \theta & \pm \cos \theta & 0 \\ 0 & 0 & s \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} e \\ f \\ o \end{pmatrix} \end{aligned} \quad (2)$$

【0037】この式を、

$$A = \begin{pmatrix} \cos \theta & \mp \sin \theta & 0 \\ \sin \theta & \pm \cos \theta & 0 \\ 0 & 0 & s \end{pmatrix}, C = \begin{pmatrix} e \\ f \\ o \end{pmatrix} \quad (3)$$

を用いて表現すると次のようになる。

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = A \begin{pmatrix} x \\ y \\ z \end{pmatrix} - C. \quad (4)$$

ここで、行列Aの(3,3)の要素sについて、s=0となるのは次の場合である。

【0038】(1) $p_x, y = c$ (cは定数、 $x = 1, \dots, B, y = 1, \dots, B$) が成立する場

ら抽出される署名画像の劣化の程度との間に正の相関関係がある、すなわち、攻撃による劣化の程度が大きくなるに従って署名画像の劣化が大きくなる。

【0034】本発明による著者認証システムが条件(i)を満足することを以下説明する。認証パラメータから生成される署名画像は、図2を用いて説明したようなレンジブロックの集合である。また、各レンジブロックは、それに対応する縮小ドメインブロック（著作画像を構成するブロックを縮小したもの）から、著者認証システムによって算出される。

【0035】したがって、条件(i)を満足することは、互いに相違するドメインブロックから同一のレンジブロックを生成しないことを証明することに等しい。さらには、著者認証システムに逆変換の存在が証明されると、互いに相違するドメインブロックから同一のレンジブロックを生成しないことが保証される。以下、著者認証システムの逆変換の存在を証明する。

【0036】レンジブロックの画素 p_x, y (ただし、座標 (x, y) 、画素値 z) と縮小ドメインブロックの画素 g_x, y (ただし、 (x', y') 座標、画素値 z') の関係を示す式は、次のように表現される。

【数1】

【数2】

【数3】

合。

(2) $g_x, y = 0$ ($x = 1, \dots, B, y = 1, \dots, B$) である縮小ドメインブロックが最良の近似を与えるブロックとして選択した場合。

【0039】(2)で示される縮小ドメインブロックが選択された場合、 $s = 0$ として、計数 o で近似すると、近似精度を変えることなく $s = 0$ が算出される事態を回避することができる。

【0040】さらに、署名画像を、(1)の場合を回避

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = A^{-1} \left(\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} - C \right)$$

が実現され、本発明による署名認証システムの逆行列の存在が保証され、条件(i)が証明された。

【0041】次に、条件(ii)を証明する。条件(ii)の証明の前に、証明で用いる文字の定義を以下のように行う。

- (1) G : 著作画像。
- (2) G', G'' : G に対してそれぞれ互いに相違する画像処理を施した2種類の画像。
- (3) G_j, G'_j, G''_j : G, G', G'' のドメインブロック。
- (4) P, P', P'' : 同一の認証パラメータを有す

$$MSE(P, P') = \sum_{i=1}^n \sum_{x=1}^B \sum_{y=1}^B (p_{i,xy} - p'_{i,xy})^2$$

$$MSE(P, P'') = \sum_{i=1}^n \sum_{x=1}^B \sum_{y=1}^B (p_{i,xy} - p''_{i,xy})^2$$

さらに、式(1)から、

$$\begin{aligned} p_{i,xy} &= s g_{k_{xy}} + o \\ p'_{i,xy} &= s g'_{k_{xy}} + o \\ p''_{i,xy} &= s g''_{k_{xy}} + o \end{aligned} \tag{7}$$

が成立する。ただし、著者認証システムによって P_i が生成されるために選択される縮小ドメインブロックを G_k とする。

$$\begin{aligned} MSE(P, P') &= s^2 \sum_{i=1}^n \sum_{x=1}^B \sum_{y=1}^B (g_{k_{xy}} - g'_{k_{xy}})^2 \\ &= s^2 MSE'(G, G') \\ MSE(P, P'') &= s^2 \sum_{i=1}^n \sum_{x=1}^B \sum_{y=1}^B (g_{k_{xy}} - g''_{k_{xy}})^2 \\ &= s^2 MSE'(G, G'') \end{aligned} \tag{8}$$

ただし、 $MSE'(G, G')$ は、署名画像を作成する際に選択された縮小画像 G と G' のドメインブロックのMSEの和を表す。

【0044】式(8)から、 $MSE'(G, G') > MSE'(G, G'')$ の場合、 $MSE(P, P') > MSE(P, P'')$ が成立する。したがって、条件(ii)が成立するためには、署名画像を作成する際に選択される縮小ドメインブロックが、著作画像全体を網羅

して作成するものとする。これによって、全てのレンジブロックについて $s = 0$ が成立し、 A の行列式 $\det A = \pm s$ から、逆行列 A^{-1} が常に存在する。逆行列 A^{-1} が存在すると、

【数4】

$$(5)$$

る著者認証システムによって G, G', G'' から生成した署名画像。

(5) P_i, P'_i, P''_i : P, P', P'' のレンジブロック。

(6) $p_{i,xy}, p'_{i,xy}, p''_{i,xy}$: P_i, P'_i, P''_i における座標 (x, y) の画素値。

(7) $g_{i,xy}, g'_{i,xy}, g''_{i,xy}$: G_i, G'_i, G''_i における座標 (x, y) の画素値。

【0042】画像 P', P'' と署名画像 P のMSEはそれぞれ次式で表現される。

【数5】

$$(6)$$

【0043】式(6)の右辺は、式(7)によって次のように変形される。

【数6】

している必要がある。

【0045】しかしながら、著作画像中にその著作物の特徴を顕著に表現していると考えられる部分がある場合については、その部分のみを縮小ドメインブロックとして選択するよう操作することによって、実質的には条件(ii)が満足される。

【0046】以上説明したように、本発明は条件(i), (ii)を満足するので、著者認証の際に用いる

ことができる。

【0047】次に、本発明の有効性を検証するために行った計算機シミュレーションの結果を説明する。計算機シミュレーションを行うに当たり、図3に示すような著作画像と、図4A及び4Bに示すような署名画像を使用した。

【0048】著作画像及び署名画像のサイズを、共に256×256画素256階調の濃淡画像とする。また、認証パラメータを算出する際のレンジブロック及びドメインブロックのサイズをそれぞれ、8×8画素及び16

$$PSNR = 10 \times \log_{10} \left(\frac{255}{MSE} \right)^2$$

$$MSE = \frac{1}{255} \sqrt{\sum_{x=1}^{255} \sum_{y=1}^{255} (Z(x,y) - Z'(x',y'))^2}$$
(9)

【0051】先ず、図3に示すような著作画像並びに図4A及び4Bに示すような署名画像を用いて、署名画像を生成するための認証パラメータをそれぞれ算出し、それをメモリに保持する。

【0052】次いで、算出された認証パラメータと、著者であることを主張したい画像としての図3に示すような画像とを用いて、署名画像を生成する。生成された署名画像を図5A及び5Bに示す。

【0053】生成された図5A及び5Bに示す署名画像の画質をPSNRによって評価すると、それぞれ22.68dB及び23.67dBとなった。したがって、生成された署名画像の画質が低下していることがわかる。画質が低下する理由は、署名画像生成部2(図1B)の性質上、生成される署名画像の品質が下がってしまうからである。

【0054】しかしながら、本発明によれば、著作画像の特徴を表現する認証パラメータを算出し、それに基づいて署名画像生成部2(図1B)から署名画像を生成している。したがって、本発明を用いることによって、著作画像の品質を保持したまま画像が提供されるという利点が得られる。

【0055】次に、平滑化フィルタ処理による影響について説明する。一般に、透かしへの攻撃方法の一つとして、画像中の雑音除去などに使用される平滑化フィルタが挙げられる。ここでは、その線形フィルタの例として平均値フィルタを使用するとともに非線形フィルタの例としてメディアンフィルタを使用した実験を行った。この場合、フィルタ窓のサイズを共に3×3とし、平均値フィルタでは、注目画素とその近傍の輝度値の重みを同一にした。

【0056】図3に示すような著作画像にこれらの平滑化フィルタ処理を施した後に本発明によって署名画像を生成した結果を図6A及び6Bに示す。

【0057】生成された図6A及び6Bに示す署名画像

×16画素とした。

【0049】ここで、レンジブロック及びドメインブロックのサイズをそれぞれ元の1/2にすると、保持すべき認証パラメータのデータ量は約4倍となり、それに伴い、著者認証システムによって生成される署名画像の画質は向上する。

【0050】計算機シミュレーションでは、画質を評価するために、次式で定義されるPSNRを用いた。

【数7】

の画質をPSNRによって評価すると、それぞれ22.35dB及び23.53dBとなった。したがって、生成された署名画像の画質は、図5A及び5Bに示す署名画像の画質とほとんど変わらないことがわかる。

【0058】すなわち、本発明は、平滑化に対して画質を画質を維持していると考えられる。これは、本発明による著者認証システムが画像の形状(各画素の輝度値の大小関係)に着目しているため、平滑化処理によって輝度値に変化が生じたとしても、その形状は大きく変化しないからである。これらの結果から、本発明は平滑化フィルタ処理に対して十分な耐性を有すると言える。

【0059】次に、JPEG圧縮による影響について説明する。画像のデータ量は比較的大きいので、画像を蓄積・配信する際にJPEG方式による圧縮が施される場合が多いが、そのような非可逆符号化によって署名が消失することは望ましくない。

【0060】図3に示す著作画像に3通りのJPEG圧縮(75%、25%及び25%の品質)を施し、生成される署名画像に及ぼされる影響を調査した。図3に示すような著作画像にこれらの平滑化フィルタ処理を施した後に本発明によって署名画像を生成した結果を図7A(75%の品質)及び6B(25%の品質)に示す。

【0061】生成された図7A及び7Bに示す署名画像の画質をPSNRによって評価すると、それぞれ22.65dB及び22.45dBとなった。なお、50%の品質の場合のPSNRは22.61dBとなった。

【0062】その結果、著作画像にJPEG圧縮を施したことによる影響は、生成された署名画像にほとんど見られないことがわかる。このことは、周波数利用型の電子透かしでは得られない。したがって、本発明はJPEG圧縮に対しても優れた特性があることがわかる。この特徴も、署名画像生成部2(図1B)の性質に起因するものであると考えられる。

【0063】次に、スケール変換による影響について説

明する。様々な画像関連のソフトウェアの開発によって画像編集が容易になっていることに伴い、画像が拡大・縮小されて利用されることが考えられる。したがって、そのような場合においても署名画像を生成できる必要がある。

【0064】線形補間法によって著作画像を垂直方向及び水平方向にそれぞれ同一倍率で拡大・縮小した後、本発明によって署名画像を生成する実験を行った。ここでは、図3に示す著作画像を0.5倍に縮小した場合(128×128画素)と、2倍に拡大した場合(512×512画素)について調査した。ただし、署名画像を署名画像生成部2(図1B)によって生成するために、図8Aに示すような縮小画像を、図8Bに示すように著作画像と同一サイズに拡大した。

【0065】著作画像を0.5倍に縮小変換した後に本発明によって生成される署名画像を図9Aに示すとともに、著作画像を2倍に拡大変換した後に本発明によって生成される署名画像を図9Bに示す。生成された図9A及び9Bに示す署名画像の画質をPSNRによって評価すると、それぞれ22.17dB及び22.63dBとなった。これらPSNRは、図4Aに示す署名画像のPSNRにほぼ等しいといえる。その結果、スケール変換に対する本発明の有効性が確認できる。

【0066】次に、周囲の切り取りによる影響について説明する。静止画像は、そのままの状態ではなく図10に示すように周囲が切り取られた状態で利用される場合もある。そのような場合についての検討を行う。なお、図10に示す画像は、25画素に相当する周囲が切り取られている。

【0067】この場合、署名画像を署名画像生成部2(図1B)によって生成する際に、切り取られた画像のサイズを著作画像と同一サイズ(256×256画素)にする必要がある。したがって、図10に示すような周囲が切り取られた画像を用いて、著作画像に対するブロックマッチングを行うことによって、切り取られた画像の著作画像における位置を推定する。

【0068】次に、全ての画素の輝度を255とする画像(256×256画素)を用意し、推定した位置情報に基づいて、用意した画像の対応する画素の輝度値を、周囲が切り取られた画像の輝度値に置換する。この操作によって生成された画像を、署名画像生成部2(図1B)への入力画像(256×256画素)として実験を行った。

【0069】図10に示すように25画素に相当する周囲が切り取られた著作画像を用いて本発明によって生成される署名画像を図11Aに示す。生成された図11Aに示す署名画像の画質をPSNRによって評価すると、15.63dBとなった。その結果、生成された画像が劣化し、署名画像としての役割を果たしていないことがわかる。このような事態を回避する方法を以下説明す

る。

【0070】これまでの説明では、署名画像の各レンジブロックに対する最良の近似を与えるドメインブロックを求めるための探索領域を、著作画像の全域としてきた。そのために、著作画像の周囲の画素が取り除かれることによって、署名画像を生成するために必要な要素が消失し、図11Aに示すように署名画像を正確に生成できなかったと考えられる。これを踏まえた上で改良法を説明する。

【0071】一般に、画像においては、中央部が視覚的に最も重要な場所となる。したがって、その領域の画素は取り除かれないと考えられるので、著作画像の中央部をドメインブロックの探索領域(70×70画素)として、認証パラメータを算出する。

【0072】このような改良法による有効性を示すために、図10に示すように25画素に相当する周囲が切り取られた著作画像を用いて署名画像を生成した。改良法によって生成される署名画像を図11Bに示す。生成された図11Bに示す署名画像の画質をPSNRによって評価すると、20.52dBとなった。

【0073】図11Bに示す署名画像では、文字の周囲がぼやけたり、黒い点のノイズが生じている。これは、ドメインブロックの探索領域が256×256画素から70×70画素に狭まったためにレンジブロックと縮小ドメインブロックとの近似が探索領域を著作画像全体とした場合に比べて悪化しているためと推定される。しかしながら、得られるPSNRからわかるように、この改良法によって、署名画像の画質は図11Aよりも向上している。

【0074】別の改良法として、署名画像に複数の同一署名を用いることによって、署名の一部が正確に生成できなくても、署名の足し合わせによって署名を合成させて、攻撃に対する耐性を持たせる方法がある。

【0075】この改良法を説明するために、図12に示すように、便宜的に署名画像6及び著作画像7を4分割し、それぞれの領域に対して番号1-4及び記号a-dを付した。これに伴い、4分割した署名画像の領域1-4がそれぞれ同一署名となるように、図4Bに示すような署名画像を用意した。

【0076】次に、認証パラメータ算出の際に、それぞれの署名(領域1-4)に関するパラメータを、互いに相違するドメインブロック探索領域a-dから算出するようにし、例えば、署名画像の領域1に位置する署名を生成するために必要なパラメータを著作画像の領域aから算出する。また、署名画像生成部2(図1B)では、生成される署名画像をそれぞれ足し合わせることによって署名画像を合成する。

【0077】このような改良法による有効性を示すために、図10に示すように25画素に相当する周囲が切り取られた著作画像を用いて署名画像を生成した。署名画

像合成前の状態を図 13A に示す。ただし、算出した認証パラメータにより、レンジブロックに対して最良の近似を与えるドメインブロックの位置が取り除かれた範囲の場合は、そのレンジブロックに対して署名画像生成部 2 (図 1B) による輝度値の生成は行わず、そのブロックを輝度値 255 で補間した。

【0078】図 13A では、画素を取り除いた影響によって部分的に署名画像が欠落しているが、領域 1 - 4 の生成された署名画像は、それぞれ互いに相違するドメインブロック探索領域 a - d から生成されるので、署名画像の欠落する位置が互いに相違すると考えられる。

【0079】このことを利用して、領域 1 - 4 の生成された署名画像をそれぞれ足し合わせた。その結果を図 13B に示す。ただし、足し合わせた輝度値が 100 以下の場合には輝度値を 0 とし、それ以外の場合には 255 とした。その結果、この改良法は、著作画像の周囲の切り取りに対する耐性があることを示す。

【0080】以上の説明から明らかなように、本発明によれば、著作画像の品質を下げることなく著者の認証を行うことができるようになり、かつ、JPEG 圧縮、平滑化及びスケール変換に対する耐性が、従来行われているような著作画像に署名を埋め込む手法よりも高くなる。また、著作画像の周辺が切り取られた場合でも、ドメインブロック探索領域の設定を適切に行うことによって、署名画像の画質の低下を防止することができる。

【0081】本発明は、上記実施の形態に限定されるものではなく、幾多の変更及び変形が可能である。例えば、上記実施の形態では画像について説明したが、文書や音声のような他のデータについても本発明を適用することができる。この場合、同一文書や同一音声と認識される程度の劣化が生じたとしても同一であると認められる。

【0082】認証パラメータを IFS パラメータ以外のパラメータとすることができ、署名画像生成部 2 による署名画像の生成を、IFS 以外に基づいて行うことがで

き、かつ、認証パラメータを、フラクタル符号化以外の手法によって算出することができる。

【図面の簡単な説明】

【図 1】 本発明による著者認証システムを説明するための図である。

【図 2】 認証パラメータの算出過程を説明するための図である。

【図 3】 著作画像の一例を示す図である。

【図 4】 署名画像の例を示す図である。

【図 5】 本発明によって生成された署名画像の例を示す図である。

【図 6】 平滑化フィルタ処理後に本発明によって生成された署名画像の例を示す図である。

【図 7】 JPEG 圧縮後に本発明によって生成された署名画像の例を示す図である。

【図 8】 著作画像のスケール変換の例を示す図である。

【図 9】 スケール変換後に本発明によって生成された署名画像の例を示す図である。

【図 10】 周囲が切り取られた著作画像の一例を示す図である。

【図 11】 周囲が切り取られた著作画像を用いた場合に本発明及びその改良法によって生成された署名画像の例を示す図である。

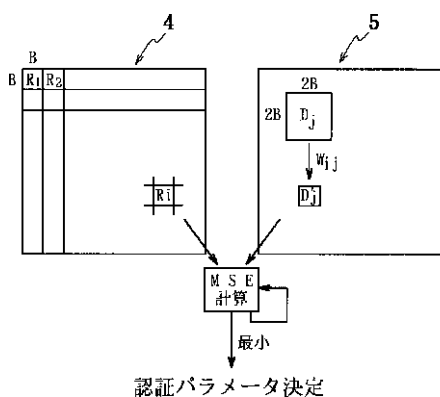
【図 12】 署名画像のレンジブロックと著作画像のドメインブロックとの関係を説明するための図である。

【図 13】 周囲が切り取られた著作画像を用いた場合に本発明の改良法によって生成された署名画像の例を示す図である。

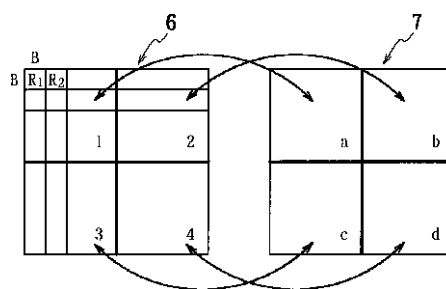
【符号の説明】

- 1 認証パラメータ算出部
- 2 署名画像生成部
- 3 署名画像照合部
- 4, 6 署名画像
- 5, 7 著作画像

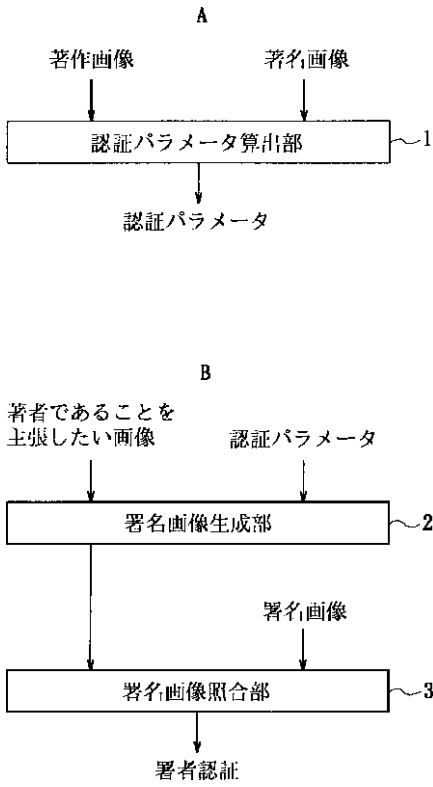
【図 2】



【図 12】



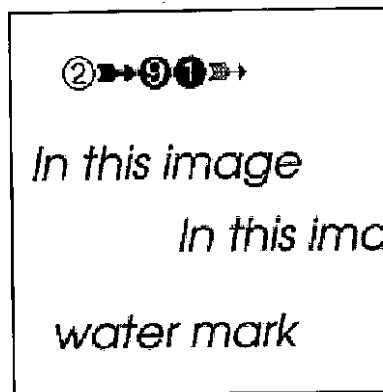
【図1】



【図3】

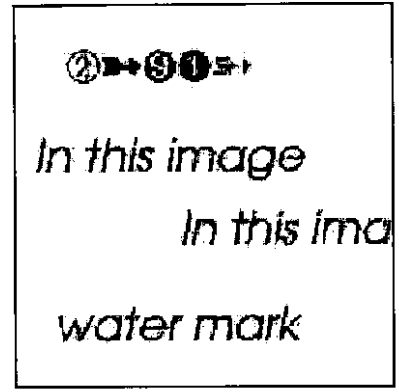


【図4】

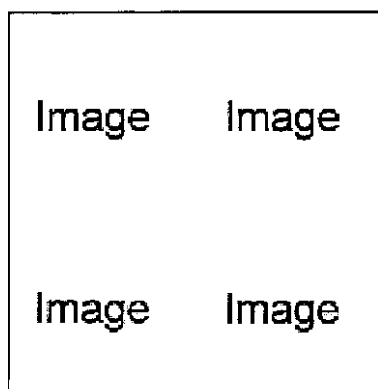


A

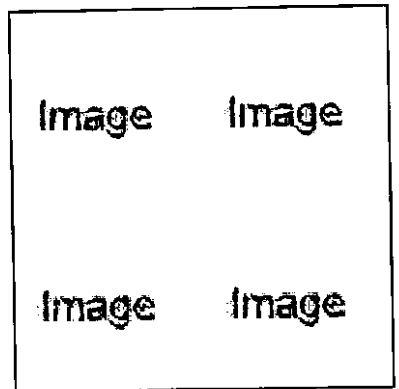
【図5】



A

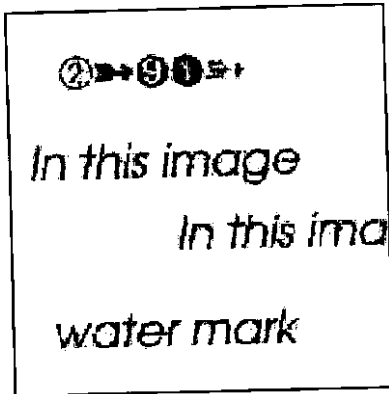


B



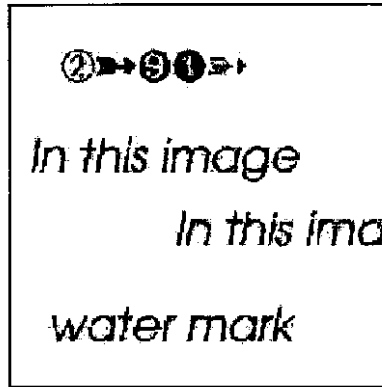
B

【図6】



A

【図7】

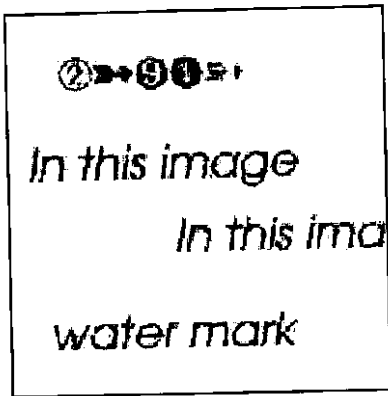


A

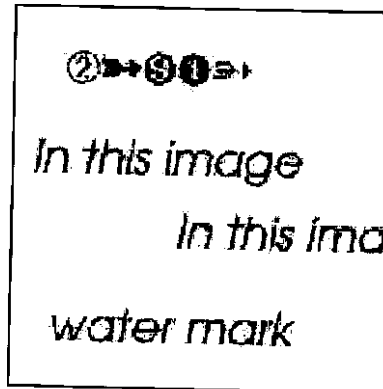
【図9】



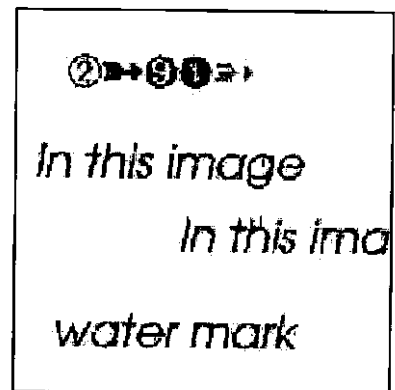
A



B



B



B

【図10】



【図8】

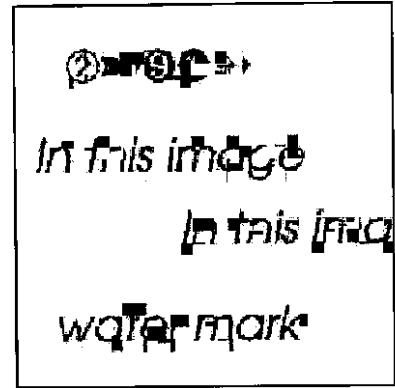


A

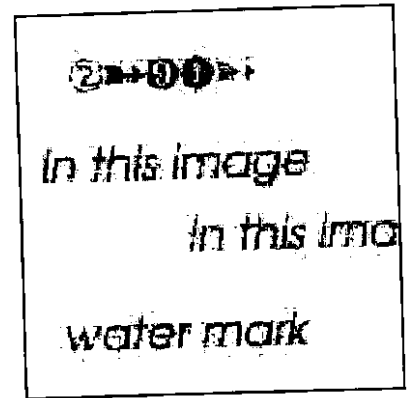


B

【図11】

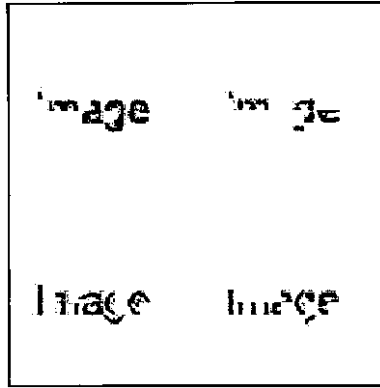


A

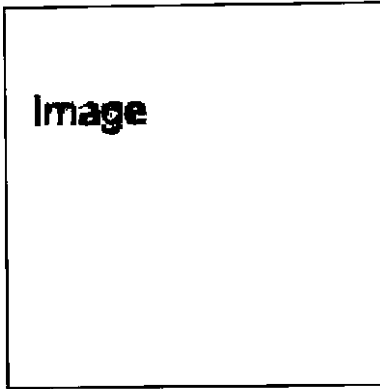


B

【図13】



A



B