(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2008-22372
(P2008-22372A)
(43)公開日　平成20年1月31日(2008.1.31)

(51)Int.Cl.			F I			テーマコード（参考）
H04N	1/387	(2006.01)	H04N	1/387		5C076
G09C	1/00	(2006.01)	G09C	1/00	640D	5J104

審査請求 未請求　請求項の数 12　ＯＬ　（全 11 頁）

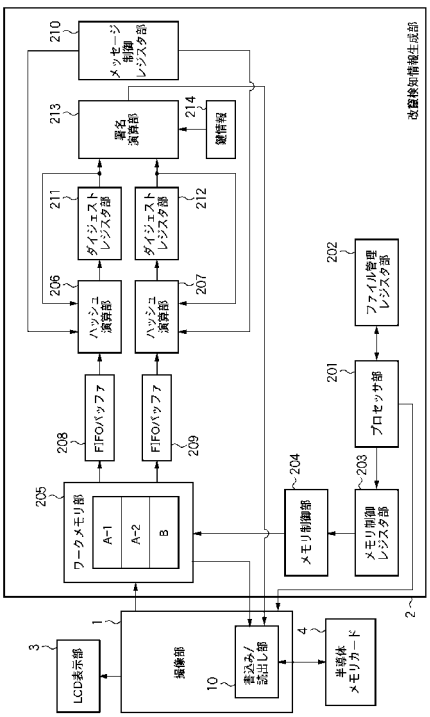
(21)出願番号　特願2006-193231 (P2006-193231)
(22)出願日　平成18年7月13日 (2006.7.13)

(71)出願人　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　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　平井　雄一
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

Ｆターム(参考)　5C076 AA01　AA14　AA36　AA40　BA06
5J104 LA01　LA05　PA14

(54)【発明の名称】改竄検知情報生成装置、撮像装置、改竄検知情報生成方法、プログラムおよび記憶媒体

(57)【要約】
【課題】改竄検出用ダイジェスト値の生成を高速に処理する。
【解決手段】画像ファイルデータを格納するメモリ手段と、メモリ手段に格納された画像ファイルデータに含まれる画像データを複数の分割画像データに分割する画像データ分割手段と、複数の分割画像データに対応し、並列的に動作してハッシュ演算を行う複数のハッシュ演算手段と、を備え、複数のハッシュ演算手段より、複数の分割画像データに対応した複数のダイジェスト値を得る改竄検知情報生成装置。
【選択図】図２



【特許請求の範囲】
【請求項１】
画像ファイルデータを格納するメモリ手段と、
前記メモリ手段に格納された前記画像ファイルデータに含まれる画像データを複数の分割画像データに分割する画像データ分割手段と、
前記複数の分割画像データに対応し、並列的に動作してハッシュ演算を行う複数のハッシュ演算手段と、を備え、
前記複数のハッシュ演算手段より、前記複数の分割画像データに対応した複数のダイジェスト値を得る、ことを特徴とする改竄検知情報生成装置。
【請求項２】
前記画像ファイルデータは、複数または単独の画像データ及びヘッダデータと、を含むことを特徴とする請求項１に記載の改竄検知情報生成装置。
【請求項３】
署名演算手段をさらに備え、
前記署名演算手段は、前記複数のダイジェスト値に対して鍵情報により署名を行い、前記画像ファイルデータに関連する署名データを生成する、ことを特徴とする請求項１又は２に記載の改竄検知情報生成装置。
【請求項４】
撮像部と、
改竄検知情報生成部と、を備え、
前記改竄検知情報生成部は、
前記撮像部で撮像して得られた画像ファイルデータを格納するメモリ手段と、
前記メモリ手段に格納された前記画像ファイルデータに含まれる画像データを複数の分割画像データに分割する画像データ分割手段と、
前記複数の分割画像データに対応し、並列的に動作してハッシュ演算を行う複数のハッシュ演算手段と、を備え、
前記複数のハッシュ演算手段より、前記複数の分割画像データに対応した複数のダイジェスト値を得る、ことを特徴とする撮像装置。
【請求項５】
前記画像ファイルデータは、複数または単独の画像データ及びヘッダデータと、を含むことを特徴とする請求項４に記載の撮像装置。
【請求項６】
前記改竄検知情報生成部は、署名演算手段をさらに備え、
前記署名演算手段は、前記複数のダイジェスト値に対して鍵情報により署名を行い、前記画像ファイルデータに関連する署名データを生成する、ことを特徴とする請求項４又は５に記載の撮像装置。
【請求項７】
取り外し可能な記憶手段に対してデータの読出し／書込みを行う読出し／書込み手段をさらに備え、
前記読出し／書込み手段は、前記取り外し可能な記憶手段に、前記画像ファイルデータと前記画像ファイルデータに関連する署名データとを書込む、ことを特徴とする請求項６に記載の撮像装置。
【請求項８】
前記画像ファイルデータに含まれる画像データを複数の分割画像データに分割する画像データ分割工程と、
前記複数の分割画像データに対応し、並列的に動作してハッシュ演算を行うハッシュ演算工程と、を備え、
前記ハッシュ演算工程により、前記複数の分割画像データに対応した複数のダイジェスト値を得る、ことを特徴とする改竄検知情報生成方法。
【請求項９】

前記画像ファイルデータは、複数または単独の画像データ及びヘッダデータと、を含むことを特徴とする請求項８に記載の改竄検知情報生成方法。
【請求項１０】
署名演算工程をさらに備え、
前記署名演算工程は、前記複数のダイジェスト値に対して鍵情報により署名を行い、前記画像ファイルデータに関連する署名データを生成する、ことを特徴とする請求項８又は９に記載の改竄検知情報生成方法。
【請求項１１】
請求項８乃至１０のいずれか１項に記載された改竄検知情報生成方法の各工程をコンピュータに実行させるプログラム。
【請求項１２】
請求項８乃至１０のいずれか１項に記載された改竄検知情報生成方法の各工程をコンピュータに実行させるプログラムが記憶されたコンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、画像データに対する改竄検知情報の生成を高速に処理可能な改竄検知情報生成装置、改竄検知情報生成装置を搭載した撮像装置、改竄検知情報生成方法、プログラムおよび記憶媒体に関する。
【背景技術】
【０００２】
従来よりよく知られているように、ＣＣＤやＣ－ＭＯＳ等の半導体撮像素子を備えるデジタルカメラにおいては、動画像信号、静止画像信号等を映像信号として取り込み、デジタル化し、画像データとして半導体メモリ等の記憶手段に格納する機能を有する。最近では、半導体技術の向上により、画素数が、例えば６００万画素から、大きいものでは１０００万画素を越える画素数を有する半導体撮像素子が開発され、使用されつつある。したがって、このような画素数の大きな半導体撮像素子を備えたデジタルカメラで撮影して得られる画像データの品質の向上は著しい。その結果、従来より使われてきた銀塩カメラの利用分野にも進出する場合が出てきている。例えば、新聞や雑誌に掲載される写真の撮影や、証明用写真等にもデジタルカメラが使われ始めている。
【０００３】
その様なデジタルカメラの利用分野の拡大に伴い、配布物としての写真の取り扱いや、写真そのものの信憑性などに注意を払うべき問題に焦点が当てられている。即ち、画像データは電気信号なので、銀塩カメラで作成した写真より容易に改竄することが可能であり、この問題を解決しないと、画像データの信憑性が疑われ、公式な証拠として採用出来ない。
【０００４】
デジタルカメラで撮影して得た画像データに対する改竄検出データの生成、署名及び記録方法の例としては、従来より幾つかの提案が為されている。例えば特許文献１には、生成した画像ファイルデータを記録媒体に保存する際、画像データは画像領域に、また署名データはプロパティ領域に格納する発明が開示されている。
【０００５】
図１は、従来技術における改竄検知情報生成回路の１例を示す。図１において、１０１は機器全体の制御を扱うプロセッサ部であり、通常ＣＰＵや、機器全体の制御を行う制御プログラムを格納するＲＯＭを含む。プロセッサ部１０１は、撮影処理、現像処理及び画像ファイルデータ生成処理を制御する。尚、図１においては、撮像処理に必要な部分は省略されている。図示しない撮像部より得られ、処理対象となる画像データは、画像ファイルデータＡ、Ｂ及びＣとして図１のワークメモリ部１０５に格納される。
【０００６】
各画像ファイルデータの属性（サイズ、格納番地等）は、図１のファイル管理レジスタ

部１０２に保持される。前記のプロセッサ部１０１は、ファイル管理レジスタ部１０２から、処理対象となる画像ファイルデータの属性を読出し、メモリ制御レジスタ部１０３へ転送する。メモリ制御レジスタ部１０３は、転送された画像ファイルデータの属性を格納する。

【０００７】

その後、メモリ制御レジスタ部１０３は、処理の対象として読み出そうとする画像ファイルデータのアドレスやサイズをメモリ制御部１０４に指示する。するとメモリ制御部１０４は、ワークメモリ部１０５に対してステータス（status）を発行し、実際にワークメモリ部１０５から画像ファイルデータを読出し、又は書き込む制御を行う。

【０００８】

図１において、１０６はハッシュ演算処理を行う為のハッシュ演算部である。ハッシュ演算処理は、改竄検出の手段として従来より一般的に使用されている。ハッシュ関数は一方向関数であり、関数の結果値より被演算データ（入力メッセージ：ここでは、画像ファイルデータである）を得る。またハッシュ演算部１０６は、演算前にプロセッサ部１０１よって初期化される必要がある。

【０００９】

ワークメモリ部１０５から読み出された画像ファイルデータは、ハッシュ演算処理を行う為にハッシュ演算部１０６へ転送される。また、１０７は署名演算部であり、たとえば、ＳＨＡ１等の演算方法が用いられる。ここでは、ハッシュ演算部１０６の演算出力結果（以下、ダイジェスト値とする）に対して、機器（たとえば、型名、製造番号などが特定されたデジタルカメラ）固有の鍵情報にて署名する働きをする。したがって、デジタルカメラ（機器）で撮影して得られた画像データ（ファイル）にそのデジタルカメラ（機器）に固有の署名データを付加することで、安全にデジタルカメラ（機器）から取り出し、外に画像ファイルデータを持ち出すことが出来る。

【特許文献１】特開２００２－０１００４４号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

図１で説明した従来技術におけるハッシュ演算部１０６では、入力となるメッセージ（画像ファイルデータ）に対して複数回の演算処理が必要となる。したがって、このハッシュ演算部１０６を通すだけでデジタルカメラとしてのスループットが低下する。例えば、ＭＤ５ Message-Digest Algorithm（以下、ＭＤ５アルゴリズムとする）では、入力メッセージの１ワードに対して４回のハッシュ演算処理が必要である。つまり、ハードウエア処理として１クロックに１回のハッシュ演算処理を行ったとしても、メッセージ（画像ファイルデータ）入力に対して４倍の処理時間が掛かることになる。その為、たとえば、高速連写を実現しているデジタルカメラ等では、高速な連写と同時に改竄検出用ダイジェスト値の生成を行う制御は、速度的に困難であった。

【課題を解決するための手段】

【００１１】

上記目的を達成するため、本発明の実施形態は、

画像ファイルデータを格納するメモリ手段と、

前記メモリ手段に格納された前記画像ファイルデータに含まれる画像データを複数の分割画像データに分割する画像データ分割手段と、

前記複数の分割画像データに対応し、並列的に動作してハッシュ演算を行う複数のハッシュ演算手段と、を備え、

前記複数のハッシュ演算手段より、前記複数の分割画像データに対応した複数のダイジェスト値を得る、ことを特徴とする改竄検知情報生成装置を提供する。

【００１２】

上記目的を達成するため、本発明の他の実施形態は、

撮像部と、

改竄検知情報生成部と、を備え、
前記改竄検知情報生成部は、
前記撮像部で撮像して得られた画像ファイルデータを格納するメモリ手段と、
前記メモリ手段に格納された前記画像ファイルデータに含まれる画像データを複数の分割画像データに分割する画像データ分割手段と、
前記複数の分割画像データに対応し、並列的に動作してハッシュ演算を行う複数のハッシュ演算手段と、を備え、
前記複数のハッシュ演算手段より、前記複数の分割画像データに対応した複数のダイジェスト値を得る、ことを特徴とする撮像装置を提供する。

【００１３】

上記目的を達成するため、本発明のさらに他の実施形態は、
前記画像ファイルデータに含まれる画像データを複数の分割画像データに分割する画像データ分割工程と、
前記複数の分割画像データに対応し、並列的に動作してハッシュ演算を行うハッシュ演算工程と、を備え、
前記ハッシュ演算工程により、前記複数の分割画像データに対応した複数のダイジェスト値を得る、ことを特徴とする改竄検知情報生成方法を提供する。

【００１４】

上記目的を達成するため、本発明のさらに他の実施形態は、前記実施形態において、改竄検知情報生成方法の各工程をコンピュータに実行させるプログラムを提供する。

【００１５】

上記目的を達成するため、本発明のさらに他の実施形態は、前記実施形態において、改竄検知情報生成方法の各工程をコンピュータに実行させるプログラムが記憶されたコンピュータ可読記憶媒体を提供する。

【発明の効果】

【００１６】

本発明によれば、対象となる画像データファイルのサイズが大きくても、改竄検出用ダイジェスト値の生成を高速に処理することが可能となる。

【発明を実施するための最良の形態】

【００１７】

＜実施形態１＞

図２は、本発明の実施形態１におけるデジタルカメラの要部ブロック図である。図２において、デジタルカメラは、撮像部１、改竄検知情報生成部２、ＬＣＤ表示部３及び取り外し可能な半導体メモリカード４とで構成される。ＬＣＤ表示部４は、撮影前の被写体画像、撮影後の被写体画像や、半導体メモリカード４に格納された画像データをモニタするために備えられる。撮像部１は、光学系、半導体撮像素子、信号処理回路、デジタル変換回路等を含み、画像データを出力する。これらの構成や動作の詳細な説明は、この明細書では省略される。

【００１８】

図２に示したデジタルカメラにおいては、撮影された画像データ（画像ファイルデータ）を複数領域に分割し、並列して同時にハッシュ値を生成し、署名する制御を行うことで高速処理を実現するものである。

【００１９】

実施形態１の説明では、改竄検知情報生成部２における画像ファイルデータのハッシュ演算処理について詳細に説明し、それ以外の撮像、現像処理等の詳細な説明等については本発明の本質ではないので省略する。

【００２０】

デジタルカメラの撮像部１で得られた画像ファイルデータＡ、Ｂは、最終的に半導体メモリカード４などの不揮発性メモリに記録されるまで、一時的格納手段としてＤＲＡＭ等の揮発性メモリに一時的に格納される。２０５は、その様な一時的格納手段としてのワー

クメモリ部を示す。当然のことながら、画像ファイルデータは、ＨＤＤ等の記録ディスク、光磁気デイスク等の記録倍他への記録のみならず、デジカルカメラに備えられた図示しないＩ／Ｆを通じて、外部にある記憶装置に転送することもありうる。

【００２１】

図２の改竄検知情報生成部２において、２０１は機器全体の制御を扱うプロセッサ部であり、通常ＣＰＵや機器全体の制御を行う制御プログラムを格納するＲＯＭを含む。プロセッサ部２０１は、撮像部１の制御も含めて、撮影処理、現像処理及び画像ファイルデータ生成処理を制御する。先に説明するように、撮像部１より得られ、処理対象となる画像データは、画像ファイルデータＡ、Ｂとして図２のワークメモリ部２０５に一時的に格納される。

【００２２】

ワークメモリ部２０５に格納された画像ファイルデータの属性（サイズ、格納番地等）は、ファイル管理レジスタ部２０２に保持される。このファイル管理レジスタ部２０２は、ワークメモリ部２０５の中に割り当てることも可能である。前記のプロセッサ部２０１は、ファイル管理レジスタ部２０２から、処理対象となる画像ファイルデータの属性を読出し、メモリ制御レジスタ部２０３へ転送する。メモリ制御レジスタ部２０３は、転送された画像ファイルデータの属性を格納する。

【００２３】

メモリ制御レジスタ部２０３は、処理の対象として読み出そうとする画像ファイルデータのアドレスやサイズをメモリ制御部２０４に指示する。するとメモリ制御部２０４は、ワークメモリ部２０５に対してステータス（status）を発行し、実際にワークメモリ部２０５から画像ファイルデータを読出し、又は書き込む制御を行う。

【００２４】

ワークメモリ２０５に画像ファイルデータＡが存在しているとする。デジタルカメラ本体の設定により改竄検出データの付加が要求されている場合、撮影して得られた画像ファイルデータＡを処理の対象となる画像ファイルデータとし、ハッシュ演算処理が施される。

【００２５】

図１で説明した従来の制御方法では、対象となる画像ファイルデータに対して一次元的にダイジェスト処理が施された。そしてＭＤ５アルゴリズム処理では、ダイジェスト値を求めるのに、１ワードに対して４回のハッシュ演算処理が行われた。ハードウエアで１クロックに１ワードを読み込んでハッシュ演算処理する場合には、最短でもその４倍の処理時間が掛かることになる。実際には、１６ワードを一対として処理され、１ワードは３２bitである。

【００２６】

本実施形態１では、２０６、２０７に示す様に、ハッシュ演算部を２つ並列に配置する。そして、対象となる画像ファイルデータＡを２つの領域（Ａ－１、Ａ－２）に分割し、分割された２つの分割画像ファイルデータＡ－１、Ａ－２に対し同時にハッシュ演算処理を実行する。これにより、対象となる画像ファイルデータＡに対する処理速度を実効的に２倍にしている。

【００２７】

すなわち、プロセッサ部２０１は、ファイル管理レジスタ部２０２より画像ファイルデータＡの属性を読み出す。画像ファイルデータＡの属性には、例えば図３（ａ）に記載された項目が含まれる。ここでは、ワークメモリ部２０５から対象となる画像ファイルデータＡを読み出す為に必要な情報（開始アドレス、データサイズ等）を選択する。

【００２８】

読み出された属性情報は、メモリ制御レジスタ部２０３に格納される。メモリ制御レジスタ部２０３には、例えば図３（ｂ）に記載の項目も格納される。図３（ｂ）中の「mode register value」とは、ワークメモリ部２０５にＳＤＲＡＭを使用した場合の（バースト数等）モード設定値である。これは、デジタルカメラ（機器）の初期動作時に設定され

る。
【００２９】
本発明の実施形態１では、プロセッサ部２０１により読出したデータ中の領域Ａ－１、Ａ－２それぞれのデータ量が算出される。算出された値にしたがって、メモリ制御レジスタ部２０３は、読出し開始アドレスとして図３中（ｂ）の読出しアドレス「read address」１、２が、また読出し量として読出し長「read length」１、２が夫々設定される。これらの設定の実行により、対象となる画像ファイルデータＡの領域を分割画像ファイルデータ領域領域Ａ－１、Ａ－２の２つの領域に分割する。
【００３０】
プロセッサ部２０１は、メモリ制御レジスタ部２０３に、ワークメモリ部２０５に対するデータ書込み／読出しの開始フラグを設定（図３（ｂ）の「write/read enable」）する。そして、メモリ制御レジスタ部２０３は、設定された開始フラグをメモリ制御部２０４へ伝達する。メモリ制御部２０４は、これを受けて、ワークメモリ部２０５に対するアクセスのステータス（status）を制御する。
【００３１】
本実施形態１では、ワークメモリ部２０５からの読出し動作を行う。メモリ制御レジスタ部２０３は、この２つの分割画像ファイルデータ領域Ａ－１、領域Ａ－２を示すアドレス値をメモリ制御部２０４に対し設定する。そして、メモリ読出しフラグを検知したメモリ制御部２０４は、交互に分割画像ファイルデータ領域Ａ－１、分割画像ファイルデータ領域Ａ－２のアドレスを更新しながらアクセスしていく。ワークメモリ部２０５より読み出された分割画像ファイルデータは、ＦＩＦＯメモリ２０８、２０９にバッファされて、それぞれ次段のハッシュ演算部２０６、２０７へ入力される。
【００３２】
通常、ワークメモリ部２０５のバス帯域は、ハッシュ演算部２０６、２０７の入力の帯域よりも広くなるように設計されるので、交互に（交番的に）読み出しても、ハッシュ演算部２０６、２０７の入力としてはほぼ同時に処理されるとみなすことが出来る。この様にして読み出された２つの分割画像ファイルデータＡ－１、Ａ－２は、ハッシュ演算部２０６、２０７へと各々入力される。
【００３３】
図２中のハッシュ演算部２０６は、演算処理の開始前に、メッセージ制御レジスタ部２１０によって初期設定が為される。設定項目は、例えば図３中（ｃ）に記載された項目を含む。図３（ｃ）中、メッセージサイズは、例えば、分割画像ファイルデータ（メッセージ）の入力後に付加されてハッシュ演算処理を実行するときに使用される。また、ダイジェスト値が４ワードから成る場合に、初期値として、word_A、word_B、word_C、word_Dがそれぞれ設定される。例えば、ＭＤ５アルゴリズムでは、
word_A : 01 23 45 67 :１６進数
word_B : 89 ab cd ef :１６進数
word_C : fe dc ba 98 :１６進数
word_D : 76 54 32 10 :１６進数
とされている。この関係は、ハッシュ演算部２０７とメッセージ制御レジスタ部２１０とでも同様な初期設定が実行される。
【００３４】
さらにメッセージ制御レジスタ部２１０においては、演算処理の開始前に、図３（ｃ）中のハッシュ処理開始フラグ「calcu enable1,2)」を有効にした状態で待機するものである。
【００３５】
また、ハッシュ演算部２０６とハッシュ演算部２０７とで処理する分割画像ファイルデータＡ－１、Ａ－２のサイズが異なる場合を想定して、前記のメッセージサイズは、各々所望の数値を設定する。
【００３６】

ハッシュ演算部２０６とハッシュ演算部２０７での計算結果は、ダイジェストレジスタ部２１１、２１２に格納される。ダイジェストレジスタ部２１１、２１２のレジスタ格納値は、例えば図３中（ｄ）に記載の項目を含む。これらダイジェスト値は、署名演算部２１３にそれぞれ供給され、たとえば、ＳＨＡ１等の演算方法で演算される。ここでは、ダイジェストレジスタ部２１１、２１２のレジスタ格納値（以下、ダイジェスト値とする）に対して、このデジタルカメラ（機器）固有の鍵情報２１４にて署名するように演算動作する。

【００３７】

かくしてダイジェスト値は、このデジタルカメラ（機器）固有の鍵情報２１４を使って署名（暗号化）され、改竄検知情報生成部２から対象となる画像ファイルデータＡに添付される。その後、撮像部１の書込み／読出し部１０により、取り外し可能な半導体メモリカード４に記憶され、デジタルカメラ外へと持ち出されることになる。

【００３８】

図４は、本発明の実施形態１の改竄検知情報生成部２の動作を説明するフローチャートであり、プロセッサ２０１に於ける本発明の要部の制御を記している。本実施形態１では、ハッシュ演算処理のメッセージである前記画像ファイルデータを分割画像ファイルデータ領域Ａ－１、Ａ－２に分割して処理する場合を１例として動作の説明をする。

【００３９】

先ず、改竄検知情報生成処理の開始後、ステップＳ４０１で、プロセッサ部２０１は、ファイル管理レジスタ部２０２より前記図３中（ａ）に記載のメモリ配置情報を取得する。次にステップＳ４０２に進み、プロセッサ部２０１は、取得したメモリ配置情報より、対象となる画像ファイルデータＡを２つの分割画像ファイルデータ領域Ａ－１、Ａ－２に分割するため、夫々のデータ量を算出する。なお、ここで分割は２つの分割画像ファイルデータ領域を同じデータ量とする等分割でも良いし、等分割でなくとも良い。

【００４０】

次に、ステップＳ４０３で、算出されたデータ量を元に、前記ワークメモリ２０５上の夫々の格納位置及び読出しデータ量を、メモリ制御レジスタ部２０３に設定する。格納位置は読出しアドレス「read address 1,2」として、データ量はサイズ「read length 1,2」として設定される。

【００４１】

さらにプロセッサ部２０１は、次のステップＳ４０４で、メッセージ制御レジスタ部２１０に対してメッセージサイズとダイジェスト初期値とを設定する。設定するメッセージ（分割画像ファイルデータ）のサイズは、ワークメモリ部２０５への読出しサイズの設定と同様に、ハッシュ演算部２０６、２０７に対して異なる値を設定することが可能である。しかしながら、ダイジェストの初期値はステップＳ４０４の設定のままとする。

【００４２】

次にプロセッサ部２０１は、ステップＳ４０５、４０６で、ハッシュ演算部２０６、２０７夫々を初期状態にした後、動作可能状態にする。図４では、先ず図３（ｃ）中の「calc(ulator) enable 1」のフラグを有効にし、続いて同図中の「calc(ulator) enable 2」のフラグを有効にする。

【００４３】

プロセッサ部２０１は、ハッシュ演算部２０６、２０７を動作可能状態にした後に、メッセージデータ（画像ファイルデータ）の読出しを要求する。図４では、ステップＳ４０７で示すように、メモリ制御レジスタ部２０３に対して、「read enable」フラグを有効にしている。

【００４４】

メモリ制御レジスタ部２０３は、このフラグの変化を検出すると、ステップＳ４０３で設定されたメモリ読出し用設定値をメモリ制御部２０４に送出すると共に、データ読出し要求（ステータス）を発行する。データ読出し要求を受けてメモリ制御部２０４は、適宜ワークメモリ部２０５の対象となる分割画像ファイルデータＡ－１、Ａ－２を読出してい

く。読み出されたデータは、ＦＩＦＯバッファ２０８、２０９に一時格納され、順次ハッシュ演算部２０６、２０７へと送出される。

【００４５】

分割画像ファイルデータ領域Ａ－１、Ａ－２へのアクセスの切り替えは、メモリ制御部２０４により制御される。この制御方法は、色々な形式で実行可能である。たとえば、１バースト単位に交互（交番的に）切り換えても良いし、ワークメモリ部２０５がＳＤＲＡＭで構成されるならば、カラム単位で切り換えても良い。

【００４６】

プロセッサ部２０１に於けるハッシュ演算の終了検知は、大抵は割込み処理により行われるが、図４のフローチャートでは、説明の簡素化の為、割り込み処理としてではなく、全体のフローチャートの一部として描いている。プロセッサ部２０１は、ステップＳ４０８におけるハッシュ演算部２０６での処理の終了と、ステップＳ４０９におけるハッシュ演算部２０７での処理の終了とを受ける。そして所望の画像ファイルデータ（ダイジェスト）が２つ（分割画像ファイルデータ領域Ａ－１とＡ－２に対応する分）得られたことを知る。

【００４７】

前記プロセッサ部２０１は、ハッシュ演算の終了を受け、ステップＳ４１０に進み、署名演算部２１３による署名演算（暗号化）の初期化を行い（得られたハッシュ値の送出、鍵情報２１４の提供等）、実行要求を出す。そして、ステップＳ４１１で署名処理が終了したことを検知し、本フローチャートは完了する。

【００４８】

署名情報として出来上がったダイジェスト値は、例えば対象とする画像ファイルデータＡの末尾に添付されて、画像ファイルデータＡと共に半導体メモリカード４に書き込まれる。そしてデジタルカメラ本体より外部へと持ち出される。半導体メモリカード４に格納された画像ファイルデータＡ（Ａ－１とＡ－２）は、パーソナルコンピュータＰＣなどの信号処理装置に装着され読み出される。このとき、ＰＣ等での展開時に、所望の鍵情報により署名情報を復号化してダイジェスト値を得ると共に、分割画像ファイルデータ領域Ａ－１及びＡ－２に対し、先に説明したものと等価のハッシュ演算処理を行って再度ダイジェスト値を得る演算を行う。そして、両者の一致を持って改竄行為がなかったことを確認する。もし、一致がなかったら、改竄された可能性を示すことになる。

【００４９】

本発明の実施形態１では、デジタルカメラに搭載された例であるが、本発明はデジタルカメラに限定されるものではない。本発明の改竄検知情報生成部は、画像読取装置（イメージスキャナ）や、医療用電子カメラ等、電子的に画像を記録する場合に、適用可能である。さらにまた、上記の説明では、画像ファイルデータが２つに分割される例を示した。しかしながら、画像ファイルデータは３つ、４つなに分割する場合も本発明は適用することが可能である。その場合には、分割数に応じてハッシュ演算部を複数設ける必要がある。たとえば、画像ファイルデータがカラー画像信号の場合、輝度信号成分（Ｙ成分）、２つの色差信号成分（Ｒ－Ｙ及びＢ－Ｙ成分）に分ける場合、または、３つのカラー信号成分（Ｒ、Ｇ及びＧ成分）に分ける場合が想定出来る。このように、分割は２つ以上でもよく、また、分割の仕方は、信号の内容で分ける場合にも本発明は適用できる。

【００５０】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給しても達成可能である。すなわち、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読出されたプログラムコード自体が前述した実施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を記憶した記憶媒体は本発明を構成することになる。

【００５１】

プログラムコードを供給するための記憶媒体としては、例えば、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、ＣＤ－Ｒ、磁気テープ、不揮発性の半導体メモリカード、ＲＯＭなどを用いることができる。また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現される場合もある。

【００５２】

しかし、さらにそのプログラムコードの指示に基づき、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）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００５３】

さらに、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードや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書込まれる場合もあり得る。その後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【図面の簡単な説明】

【００５４】

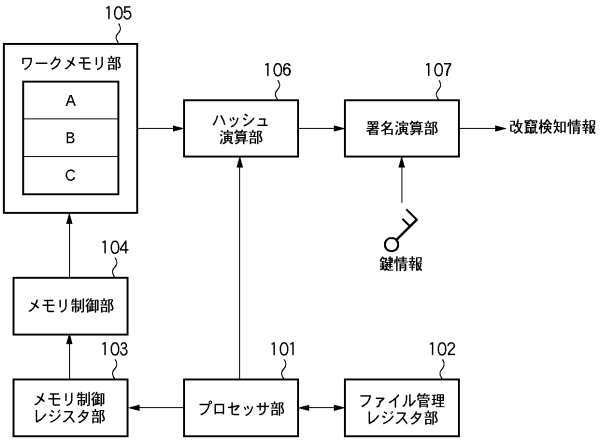
【図１】従来技術における改竄検知情報生成部の要部ブロック図である。

【図２】本発明の実施形態におけるデジタルカメラに適用した改竄検知情報生成部の要部ブロック図である。

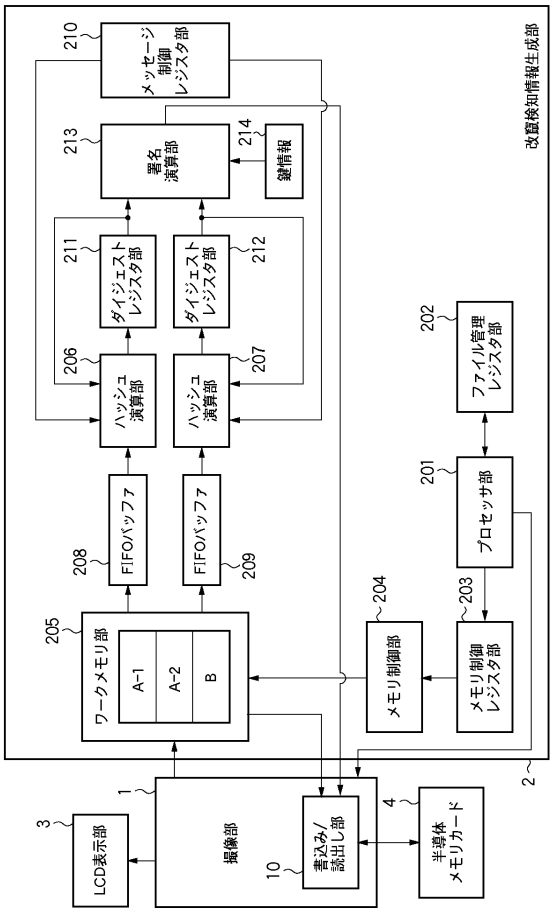
【図３】本発明の実施形態におけるデジタルカメラの改竄検知情報生成部に含まれるレジスタの内容を説明する図である。

【図４】本発明の実施形態における改竄検知情報生成部の動作を説明するフローチャートである。

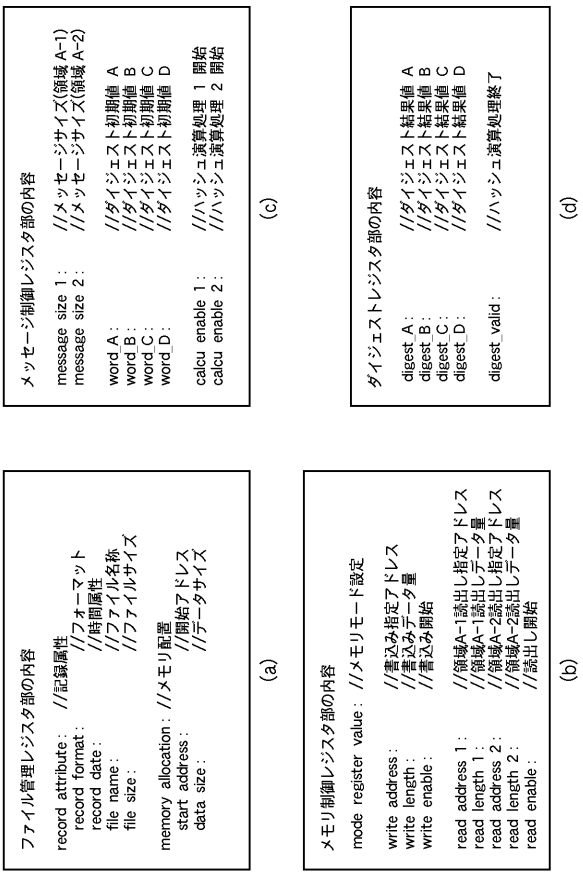
【図１】



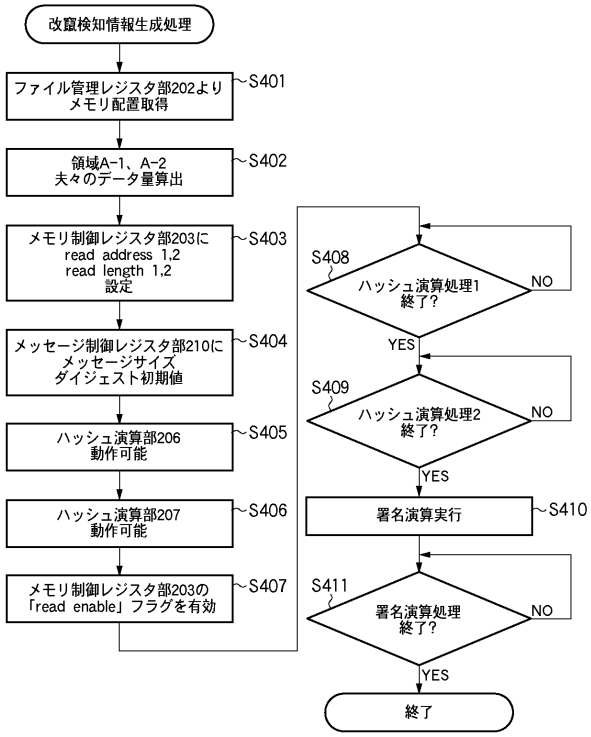
【図２】



【図３】


ファイル管理レジスタ部の内容
record attribute : //記録属性
record format : //フォーマット
record date : //時間属性
file name : //ファイル名称
file size : //ファイルサイズ
memory allocation : //メモリ配置
start address : //開始アドレス
data size : //データサイズ
(a)
メモリ制御レジスタ部の内容
mode register value : //メモリモード設定
write address : //書込み指定アドレス
write length : //書込みデータ量
write enable : //書込み開始
read address 1 : //領域A-1読出し指定アドレス
read length 1 : //領域A-1読出しデータ量
read address 2 : //領域A-2読出し指定アドレス
read length 2 : //領域A-2読出しデータ量
read enable : //読出し開始
(b)
メッセージ制御レジスタ部の内容
message size 1 : //メッセージサイズ(領域 A-1)
message size 2 : //メッセージサイズ(領域 A-2)
word A : //ダイジェスト初期値 A
word_B : //ダイジェスト初期値 B
word_C : //ダイジェスト初期値 C
word_D : //ダイジェスト初期値 D
calcu enable 1 : //ハッシュ演算処理 1 開始
calcu enable 2 : //ハッシュ演算処理 2 開始
(c)
ダイジェストレジスタ部の内容
digest A : //ダイジェスト結果値 A
digest B : //ダイジェスト結果値 B
digest_C : //ダイジェスト結果値 C
digest_D : //ダイジェスト結果値 D
digest valid : //ハッシュ演算処理終了
(d)

【図４】


改竄検知情報生成処理
ファイル管理レジスタ部202より
メモリ配置取得
S401
領域A-1、A-2
夫々のデータ量算出
S402
メモリ制御レジスタ部203に
read address 1,2
read length 1,2
設定
S403
メッセージ制御レジスタ部210に
メッセージサイズ
ダイジェスト初期値
S404
ハッシュ演算部206
動作可能
S405
ハッシュ演算部207
動作可能
S406
メモリ制御レジスタ部203の
「read enable」フラグを有効
S407
S408
ハッシュ演算処理1
終了?
NO
YES
S409
ハッシュ演算処理2
終了?
NO
YES
署名演算実行
S410
S411
署名演算処理
終了?
NO
YES
終了