【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成16年10月14日(2004.10.14)

【公開番号】特開2001-285620(P2001-285620A)
【公開日】平成13年10月12日(2001.10.12)
【出願番号】特願2000-97774(P2000-97774)
【国際特許分類第７版】
　Ｈ０４Ｎ　1/387
　Ｇ０６Ｆ　12/14
　Ｇ０９Ｃ　1/00
　Ｈ０４Ｎ　5/225
// Ｈ０４Ｎ 101:00
【ＦＩ】
　Ｈ０４Ｎ　1/387
　Ｇ０６Ｆ　12/14　３１０Ｚ
　Ｇ０９Ｃ　1/00　６４０Ｄ
　Ｇ０９Ｃ　1/00　６４０Ｂ
　Ｈ０４Ｎ　5/225　Ｚ
　Ｈ０４Ｎ 101:00

【手続補正書】
【提出日】平成15年10月6日(2003.10.6)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正の内容】
【００１７】
暗号化処理部６は、第１、第２及び第３の認証子作成手段２１、２２及び２３を有する。第１の認証子作成手段２１は、ファイルフォーマット変換部５で変換されたファイルフォーマットが入力され、これに含まれる画像データに対してハッシュ関数等の所定の関数を適用することによりメッセージ・ダイジェストＭＤを作成するメッセージダイジェスト作成部２４と、作成されたメッセージ・ダイジェストＭＤを秘密鍵メモリ１６に予め記憶された秘密鍵K_Cを用いて暗号化してメッセージ認証子ＭＡＣ１を作成し、これをヘッダ部に格納する認証子作成部２５とを有する。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正の内容】
【００１８】
第２の認証子作成手段２２は、第１の認証子作成手段２１で作成されたファイルフォーマットから画像データを抽出して画像表示部４に出力する画像データ抽出部２６と、この画像データ抽出部２６から出力される画像データに対してハッシュ関数等の所定の関数を適用することによりメッセージ・ダイジェストＭＤを作成するメッセージダイジェスト作成部２７と、作成されたメッセージ・ダイジェストＭＤを秘密鍵メモリ１６に予め記憶された秘密鍵K_Cを用いて暗号化してメッセージ認証子ＭＡＣ１’を作成する認証子作成部２８とを有する。
【手続補正３】

【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】変更
【補正の内容】
【００１９】
そして、第１の認証子作成手段２１及び第２の認証子作成手段２２で作成したメッセージ認証子ＭＡＣ１とＭＡＣ１’が認証子判定部２９に入力され、この認証子判定部２９で両者が一致するか否かを判定し、両者が不一致であるときには、データの差し替えがあったものと判断して画像データ破棄部３０で画像データを破棄する。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００２０
【補正方法】変更
【補正の内容】
【００２０】
一方、認証子判定部２９の判定結果が第１の認証子作成部２１及び第２の認証子作成部２２で作成したメッセージ認証子ＭＡＣ１とＭＡＣ１’が一致するものであるときにはゲート部３１が開かれて、画像データとメッセージ認証子ＭＡＣ１とが格納されたファイルフォーマットが第３の認証子作成手段２３に入力される。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】変更
【補正の内容】
【００２１】
この第３の認証子作成手段２３は、ゲート部３１から入力されるファイルフォーマットに基づいて画像データ及びメッセージ認証子ＭＡＣ１を含む全データに対してハッシュ関数等の所定の関数を適用することによりメッセージ・ダイジェストＭＤを作成するメッセージダイジェスト作成部３２と、作成されたメッセージ・ダイジェストＭＤを第３者秘密鍵入力手段としてＩＣカードリーダ３３から入力される第３者の秘密鍵K_{p3}を用いて暗号化してメッセージ認証子ＭＡＣ２を作成する認証子作成部３４とを有する。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００２４
【補正方法】変更
【補正の内容】
【００２４】
すなわち、改竄検査装置５０に装着された記憶媒体３８に記憶されている画像ファイルは、記憶媒体制御部５１の制御によりファイリング管理部５２に読み出される。あるいは、当該画像ファイルは通信制御部５３の制御により通信回線５４を介してファイリング管理部５２へと送られる。ファイリング管理部５２では、画像ファイルがＭＡＣ２と画像データ（この画像データには、画像データそのものの他に、ＪＰＥＧやＴＩＦＦ等のヘッダー情報を含めてもよい）とに分離され、ＭＡＣ２は第１復号化部５５に入力され、画像データはメッセージ・ダイジェスト作成部５６に入力される。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００２５
【補正方法】変更
【補正の内容】
【００２５】

第１復号化部５５では公開鍵メモリ５７にあらかじめ記憶されている第３者の秘密鍵K_{P3}に対応する公開鍵K_{P3P}を用いてメッセージ認証子ＭＡＣ２を復号化することにより、カメラの秘密鍵K_Cで暗号化されたメッセージ認証子ＭＡＣ１及び画像データを復号し、さらに、復号されたメッセージ認証子ＭＡＣ１を第２復号部５８に送られて、この第２復号部５８で公開鍵メモリ５９に予め記憶されているカメラの秘密鍵K_Cとペアとなる公開鍵K_{CP}を用いてメッセージ認証子ＭＡＣ１を復号することにより、メッセージ・ダイジェストＭＤを復号する。

【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００３１
【補正方法】変更
【補正の内容】
【００３１】
この第１の認証子作成手段２１では、メッセージダイジェスト作成部２４で画像データに対してハッシュ関数等の所定の関数を適用することにより図２（ｂ）に示すメッセージ・ダイジェストＭＤを作成し、次いで認証子作成部２５で、メッセージ・ダイジェストＭＤを秘密鍵メモリ１６に予め記憶されたカメラの秘密鍵K_Cを用いて暗号化して図２（ｃ）に示すメッセージ認証子ＭＡＣ１を作成し、このメッセージ認証子ＭＡＣ１をヘッダ部に格納して図２（ｄ）に示すファイルフォーマットを形成する。

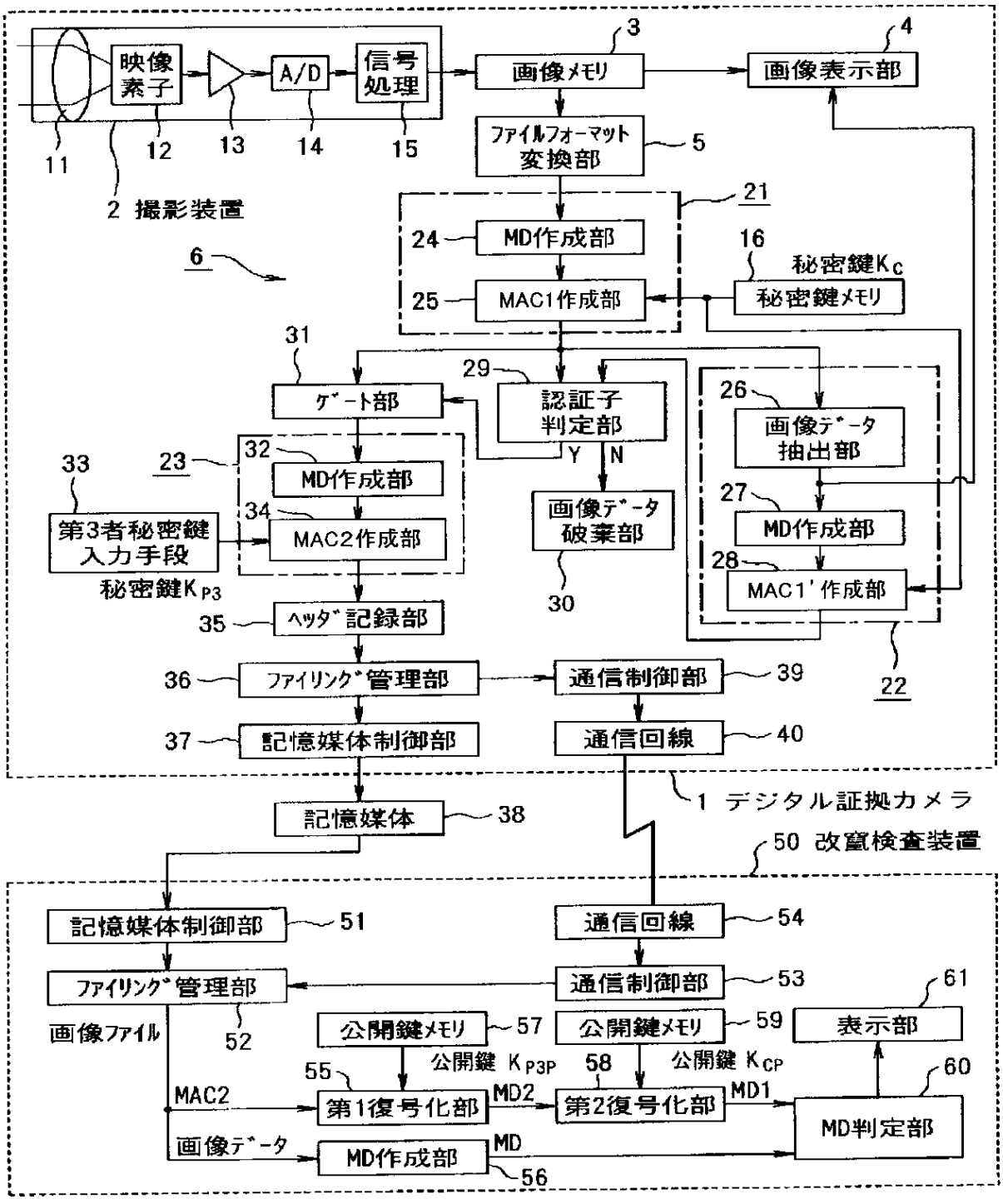
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００３４
【補正方法】変更
【補正の内容】
【００３４】
このとき、画像データ抽出部２６から画像表示部４に送られる画像データがメッセージダイジェスト作成部２７に入力されてメッセージ・ダイジェストＭＤが作成され、これがメッセージ認証子作成部２８に入力されて、秘密鍵メモリ１６に記憶されているカメラの秘密鍵K_Cを使用して暗号化されてメッセージ認証子ＭＡＣ１’が作成される。

【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００３５
【補正方法】変更
【補正の内容】
【００３５】
そして、新たに作成されたメッセージ認証子ＭＡＣ１’と第１の認証子作成手段２１で作成されたメッセージ認証子ＭＡＣ１とが認証子判定部２９に入力されて、両者が一致するか否かを判定し、両者が不一致であるときには、画像データの改竄若しくは差し替えが行われたものと判断して画像データ廃棄部３０で画像データが廃棄される。このため、改竄又は差し替えられた画像データがファイリングされることを確実に防止することができる。

【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００３６
【補正方法】変更
【補正の内容】
【００３６】
また、認証子判定部２９の判定結果が、第１及び第２の認証子作成手段２１及び２２で作成したメッセージ認証子ＭＡＣ１及びＭＡＣ１’が一致するときには、改竄又は差し替えがない正常な画像データであると判断して、第２の認証子作成手段２２で作成されたファ

イルフォーマットがゲート部３１を介して第３の認証子作成手段２３に入力される。
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００３８
【補正方法】変更
【補正の内容】
【００３８】
そして、作成されたメッセージ認証子ＭＡＣ２がファイルフォーマットのヘッダ部に更新格納されて最終的なファイルフォーマットが作成され、これがファイリング管理部３６で画像ファイルとして記憶媒体制御部３７で記憶媒体３８に格納し、この記憶媒体３８を改竄検査装置５０にセットするか又は通信制御部３９で通信回線４０を介して改竄検査装置５０に送信する。
【手続補正１３】
【補正対象書類名】図面
【補正対象項目名】図１
【補正方法】変更
【補正の内容】

【図１】


映像素子
A/D
信号処理
画像メモリ
画像表示部
ファイルフォーマット変換部
MD作成部
MAC1作成部
秘密鍵メモリ
秘密鍵Kc
撮影装置
ゲート部
認証子判定部
画像データ抽出部
MD作成部
MAC2作成部
第3者秘密鍵入力手段
秘密鍵KP3
画像データ破棄部
MD作成部
MAC1'作成部
ヘッダ記録部
ファイリング管理部
通信制御部
記憶媒体制御部
通信回線
記憶媒体
デジタル証拠カメラ
改竄検査装置
記憶媒体制御部
通信回線
ファイリング管理部
通信制御部
画像ファイル
公開鍵メモリ
公開鍵メモリ
表示部
公開鍵 KP3P
公開鍵 KCP
MAC2
第1復号化部
MD2
第2復号化部
MD1
MD判定部
画像データ
MD作成部
MD