(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7688603号
(P7688603)

(45)発行日　令和7年6月4日(2025.6.4)

(24)登録日　令和7年5月27日(2025.5.27)

(51)国際特許分類

Ｈ０４Ｌ　9/32　(2006.01)		Ｈ０４Ｌ	9/32　２００Ｂ
Ｇ０６Ｆ　21/64　(2013.01)		Ｈ０４Ｌ	9/32　２００Ｅ
		Ｇ０６Ｆ	21/64

請求項の数　19　外国語出願　（全15頁）

(21)出願番号　特願2022-72980(P2022-72980)
(22)出願日　令和4年4月27日(2022.4.27)
(65)公開番号　特開2022-174726(P2022-174726A)
(43)公開日　令和4年11月24日(2022.11.24)
審査請求日　令和7年4月23日(2025.4.23)
(31)優先権主張番号　21173288
(32)優先日　令和3年5月11日(2021.5.11)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)
早期審査対象出願

(73)特許権者　502208205
アクシス アーベー
スウェーデン国 ２２３ ６９ ルンド，グレンデン １
(74)代理人　110002077
園田・小林弁理士法人
(72)発明者　ルンドベリ， ステファン
スウェーデン国 ２２３ ６９ ルンド，グレンデン １，シー／オー アクシス コミュニケーションズ アーベー
(72)発明者　エドパルム， ヴィクトル
スウェーデン国 ２２３ ６９ ルンド，グレンデン １，シー／オー アクシス コミュニケーションズ アーベー
審査官　青木 重徳

最終頁に続く

(54)【発明の名称】　１つまたは複数のピクチャグループを含むビデオセグメントに署名するための装置および方法

(57)【特許請求の範囲】

【請求項１】

１つまたは複数のピクチャグループ（ＧＯＰ）を含むビデオセグメントに署名する方法であって、各ＧＯＰはヘッダと１つまたは複数の符号化フレームとを含み、前記方法は、

前記１つまたは複数のＧＯＰの各ＧＯＰについて、

ＧＯＰハッシュを生成すること、および

デジタル署名によって前記ＧＯＰハッシュにデジタル署名し、それによって署名付きＧＯＰハッシュを生成することと、

前記１つまたは複数のＧＯＰのうちの最後のＧＯＰを除く各ＧＯＰについて、それぞれの前記ＧＯＰのヘッダを含むそれぞれの前記ＧＯＰの任意の部分にそれぞれの前記署名付きＧＯＰハッシュを保存することはせず、その代わりに、後続のＧＯＰの前記ヘッダにそれぞれの前記署名付きＧＯＰハッシュを保存することと、

前記ビデオセグメントに対し、前記１つまたは複数のＧＯＰのうちの前記最後のＧＯＰの後に追加のＧＯＰを追加することであって、前記追加のＧＯＰはヘッダと１つまたは複数の符号化フレームとを含む、追加のＧＯＰを追加することと、

前記追加のＧＯＰの前記ヘッダに前記１つまたは複数のＧＯＰのうちの前記最後のＧＯＰの前記署名付きＧＯＰハッシュを保存することと

を含む、方法。

【請求項２】

前記追加のＧＯＰは、空のイントラフレームと０または１以上の空のインターフレーム

とを含む、請求項１に記載の方法。
【請求項３】
前記追加のＧＯＰは、前記追加のＧＯＰが前記ビデオセグメントの最後のＧＯＰであることを示す情報を含む、請求項１に記載の方法。
【請求項４】
ＧＯＰハッシュを生成することは、
前記ＧＯＰの前記１つまたは複数の符号化フレームの各符号化フレームについて、フレームハッシュを生成し、それによって１つまたは複数のフレームハッシュを生成することと、
前記１つまたは複数のフレームハッシュをハッシュし、それによって前記ＧＯＰハッシュを生成することと
を含む、請求項１に記載の方法。
【請求項５】
前記ＧＯＰハッシュを生成することは、前記１つまたは複数のフレームハッシュを、前記ビデオセグメントをキャプチャするカメラの固有の識別子および前記ビデオセグメントのタイムスタンプのうちの少なくとも一方を含むメタデータでハッシュし、それによって前記ＧＯＰハッシュを生成することをさらに含む、請求項４に記載の方法。
【請求項６】
前記１つまたは複数のフレームハッシュを前記ＧＯＰハッシュと連結し、それによって、連結されたＧＯＰハッシュを生成することをさらに含み、前記ＧＯＰハッシュにデジタル署名することは、デジタル署名によって前記連結されたＧＯＰハッシュに署名し、それによって、署名付きＧＯＰハッシュを生成することをさらに含む、請求項４に記載の方法。
【請求項７】
処理能力を有する装置で実行されたときに、請求項１から６のいずれか一項に記載の方法を実行するための命令が格納された非一時的コンピュータ可読記憶媒体。
【請求項８】
１つまたは複数のピクチャグループ（ＧＯＰ）を含むビデオセグメントに署名するための装置であって、各ＧＯＰはヘッダと１つまたは複数の符号化フレームとを含み、前記装置は、
前記１つまたは複数のＧＯＰのうちの前記ＧＯＰの各ＧＯＰについてＧＯＰハッシュを生成するように構成されたＧＯＰハッシュ生成機能と、
前記１つまたは複数のＧＯＰのうちの前記ＧＯＰの各ＧＯＰについて前記ＧＯＰハッシュにデジタル署名し、それによって前記１つまたは複数のＧＯＰのうちの前記ＧＯＰの各ＧＯＰについてそれぞれの署名付きＧＯＰハッシュを生成するように構成されたＧＯＰハッシュ署名機能と、
前記ビデオセグメントに対し、前記１つまたは複数のＧＯＰのうちの最後のＧＯＰの後に追加のＧＯＰを追加するように構成されたＧＯＰ追加機能であって、前記追加のＧＯＰはヘッダと１つまたは複数の符号化フレームとを含む、ＧＯＰ追加機能と、
前記１つまたは複数のＧＯＰの各ＧＯＰについて、それぞれの前記ＧＯＰのヘッダを含むそれぞれの前記ＧＯＰの任意の部分にそれぞれの前記署名付きＧＯＰハッシュを保存することはせず、その代わりに、後続のＧＯＰの前記ヘッダにそれぞれの前記署名付きＧＯＰハッシュを保存するように構成された署名付きＧＯＰハッシュ保存機能であって、前記１つまたは複数のＧＯＰの前記最後のＧＯＰの前記署名付きＧＯＰハッシュは、前記追加のＧＯＰの前記ヘッダに保存される、署名付きＧＯＰハッシュ保存機能と、
を実行するように構成された回路を含む、装置。
【請求項９】
前記追加のＧＯＰは、空のイントラフレームと０または１以上の空のインターフレームとを含む、請求項８に記載の装置。
【請求項１０】
前記追加のＧＯＰは、前記追加のＧＯＰが前記ビデオセグメントの最後のＧＯＰである

ことを示す情報を含む、請求項８に記載の装置。
【請求項１１】
前記ＧＯＰハッシュ生成機能は、
前記ＧＯＰの前記１つまたは複数の符号化フレームの各符号化フレームについてフレームハッシュを生成し、それによって１つまたは複数のフレームハッシュを生成することと、
前記１つまたは複数のフレームハッシュをハッシュし、それによって前記ＧＯＰハッシュを生成することと、
によってＧＯＰハッシュを生成するように構成されている、請求項８に記載の装置。
【請求項１２】
前記ＧＯＰハッシュを生成することは、前記１つまたは複数のフレームハッシュを、前記ビデオセグメントをキャプチャするカメラの固有の識別子および前記ビデオセグメントのタイムスタンプのうちの少なくとも一方を含むメタデータでハッシュし、それによって前記ＧＯＰハッシュを生成することをさらに含む、請求項１１に記載の装置。
【請求項１３】
前記１つまたは複数のフレームハッシュを前記ＧＯＰハッシュと連結し、それによって、連結されたＧＯＰハッシュを生成することをさらに含み、前記ＧＯＰハッシュにデジタル署名することは、デジタル署名によって前記連結されたＧＯＰハッシュに署名し、それによって、署名付きＧＯＰハッシュを生成することをさらに含む、請求項１１に記載の装置。
【請求項１４】
前記追加のＧＯＰは、空のイントラフレームと０または１以上の空のインターフレームとを含む、請求項７に記載の非一時的コンピュータ可読記憶媒体。
【請求項１５】
前記追加のＧＯＰは、前記追加のＧＯＰが前記ビデオセグメントの最後のＧＯＰであることを示す情報を含む、請求項７に記載の非一時的コンピュータ可読記憶媒体。
【請求項１６】
ＧＯＰハッシュを生成することは、
前記ＧＯＰの前記１つまたは複数の符号化フレームの各符号化フレームについて、フレームハッシュを生成し、それによって１つまたは複数のフレームハッシュを生成することと、
前記１つまたは複数のフレームハッシュをハッシュし、それによって前記ＧＯＰハッシュを生成することと
を含む、請求項７に記載の非一時的コンピュータ可読記憶媒体。
【請求項１７】
前記ＧＯＰハッシュを生成することは、前記１つまたは複数のフレームハッシュを、前記ビデオセグメントをキャプチャするカメラの固有の識別子および前記ビデオセグメントのタイムスタンプのうちの少なくとも一方を含むメタデータでハッシュし、それによって前記ＧＯＰハッシュを生成することをさらに含む、請求項１６に記載の非一時的コンピュータ可読記憶媒体。
【請求項１８】
前記１つまたは複数のフレームハッシュを前記ＧＯＰハッシュと連結し、それによって、連結されたＧＯＰハッシュを生成することをさらに含み、前記ＧＯＰハッシュにデジタル署名することは、デジタル署名によって前記連結されたＧＯＰハッシュに署名し、それによって、署名付きＧＯＰハッシュを生成することをさらに含む、請求項１６に記載の非一時的コンピュータ可読記憶媒体。
【請求項１９】
前記追加のＧＯＰは、空のイントラフレームと１以上の空のインターフレームとを含む、請求項７に記載の非一時的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、ビデオセグメントのコンテンツの認証に関し、具体的には、１つまたは複数のピクチャグループ（ＧＯＰ）を含むビデオセグメントに署名することに関する。
【背景技術】
【０００２】
いくつかのアプリケーションでは、ビデオセグメントのコンテンツが無傷であること、すなわちビデオセグメントのキャプチャ後に改竄されていないことを検証することが望ましい。このような検証を可能にすることは、良質の操作されたビデオを生成することを可能にするビデオ技術の発展を考慮してさらに重要になっている。１つまたは複数のピクチャグループ（ＧＯＰ）を含むビデオセグメントのそのような検証を可能にする１つの方法は、ビデオの各ＧＯＰの認証情報を作成し、ビデオセグメントの各ＧＯＰの認証情報を含めることである。次いで、認証情報は、１つまたは複数のＧＯＰの内容が無傷であることを検証するためにデコーダ側で使用され得る。しかしながら、ＧＯＰの認証情報がビデオセグメントに欠落している場合には、そのＧＯＰのコンテンツが無傷であること、すなわち改竄されていないことを確認することはできない。
【発明の概要】
【０００３】
本発明の目的は、１つまたは複数のピクチャグループ（ＧＯＰ）を含むビデオセグメントが無傷である、すなわちビデオセグメントのキャプチャ後に改竄されていないことの検証の強化を容易にすることである。
【０００４】
第１の態様によれば、１つまたは複数のＧＯＰを含むビデオセグメントに署名するための方法が提供される。各ＧＯＰは、ヘッダおよび１つまたは複数のフレームを含む。１つまたは複数のＧＯＰの各ＧＯＰについて、ＧＯＰハッシュが生成され、ＧＯＰハッシュはデジタル署名によってデジタル署名され、それにより、１つまたは複数のＧＯＰの各ＧＯＰについて署名付きＧＯＰハッシュが生成される。さらに、１つまたは複数のＧＯＰの最後のＧＯＰを除く各ＧＯＰのそれぞれの署名付きＧＯＰハッシュは、１つまたは複数のＧＯＰの後続のＧＯＰのヘッダに保存される。ビデオセグメントには、１つまたは複数のＧＯＰの最後のＧＯＰの後に追加のＧＯＰが追加される。追加のＧＯＰは、ヘッダおよび１つまたは複数のフレームを含む。次いで、１つまたは複数のＧＯＰの最後のＧＯＰの署名付きＧＯＰハッシュが追加のＧＯＰのヘッダに保存される。
【０００５】
ビデオセグメントに対し、１つまたは複数のＧＯＰの最後のＧＯＰの後にヘッダを含む追加のＧＯＰを追加し、追加のＧＯＰのヘッダ内の１つまたは複数のＧＯＰの最後のＧＯＰの署名付きＧＯＰハッシュを保存することによって、１つまたは複数のＧＯＰの最後のＧＯＰの署名付きＧＯＰハッシュがビデオセグメントに含められることが保証される。したがって、１つまたは複数のＧＯＰの最後のＧＯＰの内容が改竄されていないが、ハッシュ化および署名された内容と実際に同一であることを保証することが可能になる。
【０００６】
ＧＯＰハッシュとは、ＧＯＰのコンテンツをハッシュすることによって、または任意の同様の消化方法を使用して生成された任意の値を意味する。
【０００７】
デジタル署名によってＧＯＰハッシュにデジタル署名することは、例えば、公開／秘密鍵ペアの秘密鍵によるＧＯＰハッシュの暗号化などによって、ＧＯＰハッシュの信頼性を検証する任意の方法を意味する。
【０００８】
追加のＧＯＰに含まれる１つまたは複数のフレームは、事前符号化されてもよい。
【０００９】
追加のＧＯＰ内の１つまたは複数の事前符号化フレームを使用することにより、追加のＧＯＰをビデオセグメントの１つまたは複数のＧＯＰに追加するときに、１つまたは複数

の事前符号化フレームを符号化するための追加の時間および処理は必要とされない。

【００１０】

追加のＧＯＰは、空のイントラフレームおよび０または１以上の空のインターフレームを含むことができる。空のイントラフレームはブランクフレームであり、空のインターフレームは、別のフレームを参照し、それが参照するフレームに関連する更新を含まないフレームである。空のイントラフレームおよび任意選択的に１つまたは複数の空のインターフレームを含めることにより、追加のＧＯＰを追加するときにビデオフレームに追加される追加のビットは、空でないフレームを追加することに関連して低減される。

【００１１】

追加のＧＯＰは、追加のＧＯＰがビデオセグメントの最後のＧＯＰであることを示す情報をさらに含んでもよい。追加のＧＯＰが最後のＧＯＰであるという情報を含めることにより、デコーダ側で追加のＧＯＰを識別することができる。これは、前のＧＯＰが検証可能なコンテンツを含む最後のＧＯＰであり、指示を含む追加のＧＯＰが前のＧＯＰのコンテンツの検証を可能にするためにのみ追加されることがデコーダ側で決定され得るため、有益である。

【００１２】

ＧＯＰハッシュは、ＧＯＰの１つまたは複数のフレームの各フレームについてフレームハッシュを生成し、それによって１つまたは複数のフレームハッシュを生成し、１つまたは複数のフレームハッシュをハッシュし、それによってＧＯＰハッシュを生成することによって生成することができる。

【００１３】

１つまたは複数のフレームハッシュをハッシュしてＧＯＰハッシュを生成することにより、ＧＯＰが改竄されているかどうかを判定するために１つのハッシュのみをチェックする必要がある。

【００１４】

ＧＯＰハッシュを生成することは、ビデオセグメントをキャプチャするカメラの固有の識別子およびビデオセグメントのタイムスタンプのうちの少なくとも一方を含むメタデータで１つまたは複数のフレームハッシュをハッシュし、それによってＧＯＰハッシュを生成することをさらに含むことができる。メタデータは、ハードウェアタイプ（カメラタイプ）、ファームウェアバージョン、ＧＰＳ位置、フレームスタンプ、およびブート回数のうちの少なくとも１つをさらに含むことができる。

【００１５】

メタデータも１つまたは複数のフレームハッシュでハッシュしてＧＯＰハッシュを生成することにより、メタデータが改竄されているか否かを判定することができる。

【００１６】

１つまたは複数のフレームハッシュは、１つまたは複数のフレームハッシュをハッシュすることによって生成されたＧＯＰハッシュとさらに連結され、それによって連結されたＧＯＰハッシュを生成することができる。ＧＯＰハッシュにデジタル署名することは、デジタル署名によって連結されたＧＯＰハッシュに署名し、それによって署名付きＧＯＰハッシュを生成することをさらに含むことができる。

【００１７】

次いで、ＧＯＰが改竄されているとＧＯＰハッシュによって判定された場合には、署名付きＧＯＰハッシュの１つまたは複数のフレームハッシュを使用して、どのフレームまたはどの複数のフレームが改竄されているかを識別することができる。

【００１８】

第２の態様によれば、処理能力を有する装置で実行されると、第１の態様による方法を実施するための命令を記憶した非一時的コンピュータ可読記憶媒体が提供される。

【００１９】

第１の態様による方法の上述の任意選択の追加の特徴は、適用可能な場合、この第２の態様にも適用される。過度の繰り返しを避けるために、上記が参照される。

【００２０】
第３の態様によれば、１つまたは複数のピクチャグループＧＯＰを含むビデオセグメントに署名するための装置が提供される。各ＧＯＰは、ヘッダおよび１つまたは複数のフレームを含む。装置は、１つまたは複数のＧＯＰのうちのＧＯＰの各ＧＯＰについてＧＯＰハッシュを生成するように構成されたＧＯＰハッシュ生成機能と、１つまたは複数のＧＯＰのうちのＧＯＰの各ＧＯＰについてＧＯＰハッシュにデジタル署名し、それによって１つまたは複数のＧＯＰのうちのＧＯＰの各ＧＯＰについてそれぞれの署名付きＧＯＰハッシュを生成するように構成されたＧＯＰハッシュ署名機能と、ビデオセグメントに対し、１つまたは複数のＧＯＰのうちの最後のＧＯＰの後に追加のＧＯＰを追加するように構成されたＧＯＰ追加機能であって、追加のＧＯＰはヘッダと１つまたは複数のフレームとを含む、ＧＯＰ追加機能と、１つまたは複数のＧＯＰの各ＧＯＰについて、後続のＧＯＰのヘッダにそれぞれの署名付きＧＯＰハッシュを保存するように構成された署名付きＧＯＰハッシュ保存機能であって、１つまたは複数のＧＯＰの最後のＧＯＰの署名付きＧＯＰハッシュは、追加のＧＯＰのヘッダに保存される、署名付きＧＯＰハッシュ保存機能と、を実行するように構成された回路を含む。
【００２１】
第１の態様による方法の上述の任意選択の追加の特徴は、適用可能な場合、この第３の態様にも適用される。過度の繰り返しを避けるために、上記が参照される。
【００２２】
本発明のさらなる適用範囲は、以下に与えられる詳細な説明から明らかになるであろう。しかしながら、本発明の範囲内の様々な変更および修正がこの詳細な説明から当業者に明らかになるので、詳細な説明および特定の例は、本発明の好ましい実施形態を示しているが、単なる例示として与えられていることを理解されたい。
【００２３】
したがって、本発明は、記載された装置の特定の構成部品または記載された方法の動作に限定されず、そのような装置および方法は変化し得ることを理解されたい。本明細書で使用される用語は、特定の実施形態のみを説明するためのものであり、限定することを意図するものではないことも理解されたい。本明細書および添付の特許請求の範囲で使用される場合、冠詞「ａ」、「ａｎ」、「ｔｈｅ」、および「ｓａｉｄ」は、文脈が明らかにそうでないことを指示しない限り、１つまたは複数の要素があることを意味することを意図していることに留意されたい。したがって、例えば、「ユニット」または「前記ユニット」への言及は、いくつかの装置などを含んでもよい。さらに、「備える」、「含む」、「含有する」、および同様の表現は、他の要素またはステップを排除するものではない。
【００２４】
本発明の上記および他の態様は、添付の図面を参照してより詳細に説明される。図面は限定的であると見なされるべきではなく、説明および理解のために使用される。
【図面の簡単な説明】
【００２５】
【図１】いくつかのピクチャグループ（ＧＯＰ）を含むビデオセグメントの一例を示す図である。
【図２】１つまたは複数のＧＯＰを含むビデオセグメントに署名するための本開示の方法の実施形態に関するフローチャートを示す図である。
【図３ａ】本開示の方法の実施形態による、ビデオセグメントの最後のＧＯＰではないＧＯＰに署名することを示す図である。
【図３ｂ】本開示の方法の実施形態によるビデオセグメントの最後のＧＯＰに署名することを示す図である。
【図４】１つまたは複数のＧＯＰを含むビデオセグメントに署名するための本開示の装置の実施形態に関する概略図である。
【発明を実施するための形態】
【００２６】

本発明の現在好ましい実施形態が示されている添付の図面を参照して、本発明を以下に説明する。しかしながら、本発明は、多くの異なる形態で具体化されてもよく、本明細書に記載の実施形態に限定されると解釈されるべきではない。

【００２７】

本発明の実施形態は、デジタル署名付きＧＯＰハッシュがビデオシーケンス内の各ＧＯＰに対して作成され、各ＧＯＰのデジタル署名付きＧＯＰハッシュがビデオセグメント内の後続のＧＯＰに含められるアプリケーションにおいて、ビデオセグメントのコンテンツが無傷であること、すなわちビデオのキャプチャ後に改竄されていないことを保証するために使用され得る。デコーダ側では、ＧＯＰのデジタル署名を使用して、ＧＯＰの発信元を検証することができる。例えば、ＧＯＰ用のデジタル署名が公開／秘密鍵ペアの秘密鍵によるＧＯＰハッシュの暗号化によって作成されている場合には、署名元は、公開／秘密鍵ペアの公開鍵を使用した復号化によって検証することができる。さらに、デコーダ側で受信されたＧＯＰのコンテンツからＧＯＰハッシュを生成し、（復号化された）デジタル署名付きＧＯＰハッシュと比較することができる。それらが等しい場合には、ＧＯＰの内容は無傷であり、それらが等しくない場合には、ＧＯＰの内容は無傷ではない。さらに、そのようなアプリケーションの場合、ビデオシーケンスの最後のＧＯＰに対するデジタル署名付きハッシュは、ビデオセグメント内に最後のＧＯＰに続くＧＯＰがないため、ビデオシーケンスに含められない。したがって、最後のＧＯＰの内容が無傷であること、すなわち、キャプチャ後に改竄されていないことを保証することはできない。さらに、最後のＧＯＰがビデオセグメントの終端の前に数フレームのみを含む場合には、最後のＧＯＰの無傷であると検証できないフレームの量は少ない。しかしながら、最後から２番目のＧＯＰのデジタル署名付きＧＯＰハッシュを生成する時間は、ビデオセグメントの終端の前の最後のＧＯＰの最初の数フレームに含められることができないような時間であってもよい。したがって、そのような場合、ビデオセグメントにおいて、最後から２番目のＧＯＰにも署名付きＧＯＰハッシュは含められず、最後から２番目のＧＯＰのコンテンツも無傷であると検証することができない。そのような場合、最後から２番目のＧＯＰの署名付きＧＯＰハッシュが最後のＧＯＰに含められることが保証され得る。あるいは、最後から２番目のＧＯＰと最後のＧＯＰの両方のＧＯＰハッシュが生成され、追加のＧＯＰに含められてもよい。

【００２８】

本発明の実施形態は、ビデオセグメントのかなりの数のフレームがビデオセグメントの最後のＧＯＰ内にあるというリスクがある場合に有利である。例えば、ビデオセグメントの最後のＧＯＰの終端を考慮せずにビデオセグメントの終端が決定される場合には、ビデオセグメントの終端が所与のフレームの後にある確率は、最後のＧＯＰ内のすべてのフレームにわたって均一になる。したがって、各ＧＯＰ内のフレーム数が多いほど、ビデオセグメントの実質的な数のフレームがビデオセグメントの最後のＧＯＰ内にある確率が高くなる。最後のＧＯＰの終端を考慮せずにビデオセグメントの終わりを決定することができる一例は、ビデオセグメントが監視ビデオに関連するときであり、ビデオセグメントはトリガがアクティブになったときに開始され、トリガがアクティブになったときに終了する。そのような例では、ビデオセグメントは、現在のＧＯＰの終端に対してランダムな位置の後に終了する。したがって、各ＧＯＰに含められるフレームの数が増加するにつれて、ビデオセグメントのかなりの部分が最後のＧＯＰ内にあるリスクが増加する。さらに、トリガがアクティブになり、キャプチャがアクティブになることに関連してビデオセグメントが開始および終了されるので、ビデオセグメントの最後のＧＯＰが関心のある情報を含む可能性もある。トリガは、動きの検出、人／顔の検出、ドアが開いていることの検出などであってもよい。例えば、トリガが監視カメラによってキャプチャされたビデオ内の動きまたは人／顔である場合には、トリガは、人が監視カメラに向かって移動しているように見えるときにアクティブになり、人が監視カメラを通過したときにアクティブであることを掴むことができる。そのような場合、人物が監視カメラを通過する直前に人物の顔が監視カメラに最も近くなり、トリガがアクティブになるように、すなわちビデオセグメン

トの終端に捕捉される。したがって、顔が監視カメラに最も近く、識別が最も容易である可能性が高いフレームは、ビデオセグメントの最後から２番目または最後のＧＯＰ内にあり得る。

【００２９】

本発明の実施形態は、ビデオセグメントが１つのＧＯＰのみを含む場合にさらに有利である。この場合、１つのＧＯＰはまた最後のＧＯＰとなり、ビデオセグメントのすべてのフレームがビデオセグメントの最後のＧＯＰ内にあり、任意のフレームが関心のある情報を含む場合には、それは最後のＧＯＰ内にある。

【００３０】

図１は、本発明の実施形態に関連して使用され得るいくつかのＧＯＰ１０１～１０４を含むビデオセグメント１００の一例の図を示す。各ＧＯＰはいくつかのフレームを含み、最初のフレームはイントラフレームＩであり、その後にビデオセグメントの最初の３つのＧＯＰ１０１～１０３の６つのインターフレームＰ１～Ｐ６が続き、最後のＧＯＰ１０４の４つのインターフレームＰ１～Ｐ４が続く。ビデオセグメント１００は、例えば、最後のＧＯＰの終端を考慮せずに終了が決定されたビデオセグメント１００であってもよい。ビデオセグメントの最初の３つのＧＯＰ１０１～１０３は完全なＧＯＰであるが、最後のＧＯＰ１０４は完全なＧＯＰのフレームのサブセットのみを含むことができる。例えば、ビデオセグメント１００の最後のＧＯＰ１０４は、１つのイントラフレームＩおよび４つのインターフレームＰ１～Ｐ４を含む。ビデオセグメントが第４のインターフレームＰ４の後に終了しなかった場合には、ＧＯＰはさらなるインターフレームを含んでもよい。ビデオセグメント１００は、例えば、監視カメラ、身体装着型カメラなどのビデオカメラによってキャプチャされ、続いてエンコーダによって符号化されたビデオフレームに関することができる。

【００３１】

図１のビデオセグメント１００は簡略化された図であることに留意されたい。例えば、各ＧＯＰのインターフレームの数は、数百のインターフレームなど、図示されているよりも多くてもよく、ＧＯＰ間で異なっていてもよい。さらに、ビデオセグメントのＧＯＰの数は、ビデオセグメントの長さおよび含まれる各ＧＯＰの長さに応じて、図示した４つのＧＯＰ１０１～１０４より多くてもよい。さらに、開示された例が主にＰフレームに関連する場合であっても、本発明は、２つ以上の他のフレームを参照し得るＢフレームのような他のタイプのインター符号化フレームにも適応され、適用され得る。

【００３２】

ｎ≧１（すなわち、１つまたは複数のＧＯＰ）であり、各ＧＯＰがヘッダおよび１つまたは複数のフレームを含む、ｎ個のＧＯＰを含むビデオセグメントに署名する方法２００の実施形態を、ここで図１、図２、図３ａおよび図３ｂに関連して説明する。方法２００は、ＧＯＰハッシュを生成することＳ２１０と、デジタル署名によってＧＯＰハッシュにデジタル署名することＳ２２０と、を含み、それによって、図１のビデオセグメントなどのビデオセグメントの各ＧＯＰｉ＝１～ｎについてＳ２０８、Ｓ２２２、Ｃ２２４（すなわち、ｎ個のＧＯＰの各ＧＯＰについて）署名付きＧＯＰハッシュを生成する。

【００３３】

図３ａを参照すると、ＧＯＰｉのＧＯＰハッシュは、ＧＯＰｉのフレームＩ、Ｐ１～Ｐ６のフレームハッシュに基づくことができる。フレームのコンテンツに対するハッシュ機能Ｈを用いて、フレームのフレームハッシュが生成される。数学的ハッシュ機能の例は、アイデンティティハッシュ、フォールディング、分割ハッシュ、乗算ハッシュ、フィボナッチハッシュ、およびゾブリストハッシュである。暗号化ハッシュ機能の例は、ＭＤ５、ＳＨＡ－１、ＳＨＡ－２（ＳＨＡ－２５６／ＳＨＡ－５１２）、ＳＨＡ－３、ＢＬＡＫＥ－３である。例えば、フレームＩ、Ｐ１～Ｐ６の各々のフレームハッシュは、ＧＯＰｉのＧＯＰハッシュを生成するために、ハッシュ機能Ｈを使用して連結され３１０、次いでハッシュされてもよい。任意選択的に、メタデータＭＤはまた、ＧＯＰｉのＧＯＰハッシュを生成するために、フレームＩ、Ｐ１～Ｐ６の各々のフレームハッシュと連結されてもよ

い（３１０）。メタデータＭＤは、ビデオセグメントをキャプチャするカメラの固有識別子、ビデオセグメントのタイムスタンプ、ハードウェアタイプ（カメラタイプ）、ファームウェアバージョン、ＧＰＳ位置、フレームスタンプ、およびブート回数のうちの少なくとも１つを含むことができる。次いで、ＧＯＰハッシュは、ＧＯＰの発信元の検証を可能にする任意のタイプのデジタル署名を使用して、例えば、本方法が実行されるカメラなどの装置の公開／秘密鍵ペアの秘密鍵によるＧＯＰハッシュの暗号化を使用して、署名される３２０。例えば、ＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）２５６ビット暗号化、デジタル署名アルゴリズム（ＤＳＡ）、および楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ）は、ＧＯＰハッシュにデジタル署名するために使用され得る。

【００３４】

メタデータＭＤの有無にかかわらず、ＧＯＰｉのフレームＩ、Ｐ１～Ｐ６の１つまたは複数のフレームハッシュの連結のハッシュを使用してＧＯＰｉのＧＯＰハッシュを生成し、次いでＧＯＰハッシュにデジタル署名すること３２０によって、ＧＯＰｉの内容が無傷である、すなわち改竄されていないことの検証をＧＯＰレベルで行うことができる。あるいは、ＧＯＰｉの１つまたは複数のフレームハッシュは、ＧＯＰｉの連結されたＧＯＰハッシュを生成するために、ＧＯＰｉのＧＯＰハッシュと連結されてもよく（図３ａには図示せず）、次いで、連結されたＧＯＰハッシュは、署名付きＧＯＰハッシュを生成するために、デジタル署名によってデジタル署名される３２０。この代替形態では、ＧＯＰハッシュに関連する署名付きＧＯＰハッシュの部分を使用して、ＧＯＰの内容がＧＯＰレベルで無傷である、すなわち改竄されていないことを検証することができる。ＧＯＰが無傷ではないことが示された場合には、連結された１つまたは複数のフレームハッシュに関連する署名付きＧＯＰハッシュの一部は、デコーダ側でＧＯＰのフレームのコンテンツから生成されたフレームハッシュと比較することによって、１つまたは複数のフレームハッシュのどのフレームが改竄されているかを識別するために使用され得る。

【００３５】

さらに、ＧＯＰの並べ替えおよび検出不能なカットの識別を可能にするために、後続のＧＯＰｉ＋１の最初のフレームＩのフレームハッシュを生成し、署名前にＧＯＰｉのＧＯＰハッシュに追加することもできる。あるいは、ＧＯＰｉのＧＯＰハッシュは、ＧＯＰｉのフレームのフレームハッシュと後続のＧＯＰｉ＋１の最初のフレームＩのフレームハッシュとの連結をハッシュすることによって生成されてもよい。

【００３６】

図２に戻ると、ＧＯＰの数ｎが１よりも大きいＣ２２６（すなわち、最初のＧＯＰは唯一のＧＯＰではなく、したがって最後のＧＯＰでもない）場合には、本方法は、各ＧＯＰｉ＝１～ｎ－１についてＳ２２８、Ｓ２３２、Ｃ２３４、すなわち最後のＧＯＰを除く各ＧＯＰについて、後続のＧＯＰｉ＋１のヘッダにＧＯＰｉの署名付きＧＯＰハッシュを保存することＳ２３０をさらに含む。

【００３７】

図３ａを参照すると、ＧＯＰｉの署名付きＧＯＰハッシュは、後続のＧＯＰｉ＋１のヘッダに含められる３３０。例えば、ＧＯＰハッシュは、図３ａに示すＧＯＰｉのフレームＩ、Ｐ１～Ｐ６とは異なるメタデータフレーム（図示せず）に含められてもよい。

【００３８】

図２に戻ると、本方法は、ビデオセグメントに対し、ｎ個のＧＯＰのうちの最後のＧＯＰｎの後に追加のＧＯＰｎ＋１を追加することＳ２４０をさらに含み、追加のＧＯＰｎ＋１は、ヘッダおよび１つまたは複数のフレームを含む。次に、ｎ個のＧＯＰの最後のＧＯＰｎの署名付きＧＯＰハッシュが追加のＧＯＰｎ＋１のヘッダに保存される（Ｓ２５０）。

【００３９】

追加のＧＯＰｎ＋１は、最後のＧＯＰｎのＧＯＰハッシュが含められる限り、どのようなものであってもよい。しかしながら、ビデオセグメントのサイズを不必要に増加させず、処理に必要な処理および時間を低く保つように追加のＧＯＰｎ＋１を生成するために、ＧＯＰのサイズを可能な限り小さく保つことが有益である。

【００４０】
例えば、追加のＧＯＰに含まれる１つまたは複数のフレームは、事前符号化されてもよい。これは、１つまたは複数のフレームのコンテンツが事前に符号化されていることを意味する。１つまたは複数のプリコーディングされたフレームを使用することにより、追加のＧＯＰを追加するときにコンテンツを符号化するために追加の時間またはリソースは必要とされない。追加のフレームは、主にｎ個のＧＯＰの最後のＧＯＰｎの署名付きハッシュを搬送することを意図しているため、追加のＧＯＰ内で１つまたは複数のプリコーディングされたフレームを使用することが可能である。したがって、追加フレームのコンテンツは、ビデオフレームの他のＧＯＰのコンテンツに関連する必要はない。さらに、追加のＧＯＰｎ＋１の後には追加のＧＯＰが続かないため、追加のＧＯＰの署名付きＧＯＰハッシュを後続のＧＯＰに含めることはできず、したがって追加のＧＯＰの内容は改竄されていないと検証することはできない。
【００４１】
さらに、追加のＧＯＰの１つまたは複数のフレームは、空のイントラフレームおよび任意選択的に１つまたは複数の空のインターフレームであってもよい。空のイントラフレームは、イントラ予測のみを有し、符号化された係数を含まないブランクフレームであり、空のインターフレームは、別のフレームを参照し、それが参照するフレームに関連する更新を含まないフレームである。空のイントラフレームおよび任意選択的に１つまたは複数の空のインターフレームを含めることにより、追加のＧＯＰを追加するときにビデオフレームに追加される追加のビットは、空でないフレームを追加することに関連して低減される。
【００４２】
追加のＧＯＰは、追加のＧＯＰがビデオセグメントの最後のＧＯＰであることを示す情報をさらに含んでもよい。そのような情報は、例えば、追加のＧＯＰがビデオセグメントの最後のＧＯＰであることを示すためにデコーダで解釈することができる追加のＧＯＰのヘッダに追加のメタデータとして含められてもよい。追加のメタデータは、追加のＧＯＰが、前のＧＯＰの内容が無傷であることを検証するためにのみ使用されるべきであることを示すためにさらに使用されてもよい。これに加えて、またはこれに代えて、追加のＧＯＰがビデオセグメントの最後のＧＯＰであることを示す情報が追加のＧＯＰのコンテンツに含められてもよい。例えば、追加のＧＯＰは、ＧＯＰがビデオセグメントの最後のＧＯＰであることを示すテキストを表示するなど、符号化および表示後にＧＯＰがビデオセグメントの最後のＧＯＰであることを示すコンテンツを含む事前符号化フレームであってもよい。ヘッダに追加のメタデータを含める代わりに、それは、かすかな（基本的に不可視の）「透かし」として追加のＧＯＰのビデオデータに符号化されてもよく、フレーム外符号化データ、すなわち、フレームが終了したことが示された後で、次のフレームが開始することが示される前のデータに追加されてもよく、または未定義のネットワーク抽象化レイヤ（ＮＡＬ）に追加されてもよい。
【００４３】
図３ｂを参照すると、ＧＯＰｎのＧＯＰハッシュは、ＧＯＰｉのフレームＩ、Ｐ１～Ｐ４のフレームハッシュに基づくことができる。例えば、ＧＯＰｎのＧＯＰハッシュを生成することは、ハッシュ機能Ｈを使用して、ＧＯＰｎの各フレームＩ、Ｐ１～Ｐ４についてフレームハッシュを生成することを含むことができる。次いで、フレームＩ、Ｐ１～Ｐ４の各々のフレームハッシュを連結し３１０、ハッシュ機能Ｈを使用してハッシュして、ＧＯＰｎのＧＯＰハッシュを生成することができる。任意選択的に、メタデータＭＤはまた、ＧＯＰｎのＧＯＰハッシュを生成するために、フレームＩ、Ｐ１～Ｐ４の各々のフレームハッシュと連結されてもよい（３１０）。メタデータＭＤは、ビデオセグメントをキャプチャするカメラの固有識別子、ビデオセグメントのタイムスタンプ、ハードウェアタイプ（カメラタイプ）、ファームウェアバージョン、ＧＰＳ位置、フレームスタンプ、およびブート回数のうちの少なくとも１つを含むことができる。次いで、ＧＯＰハッシュは、ＧＯＰの発信元の検証を可能にする任意のタイプのデジタル署名を使用して、例えば、本

方法が実行されるカメラなどの装置の公開／秘密鍵ペアの秘密鍵によるＧＯＰハッシュの暗号化を使用して、署名される３２０。例えば、ＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）２５６ビット暗号化、デジタル署名アルゴリズム（ＤＳＡ）、および楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ）は、ＧＯＰハッシュにデジタル署名するために使用され得る。

【００４４】

メタデータＭＤの有無にかかわらず、ＧＯＰｎのフレームＩ、Ｐ１～Ｐ４の１つまたは複数のフレームハッシュの連結のハッシュを使用してＧＯＰｎのＧＯＰハッシュを生成し、次いでＧＯＰハッシュにデジタル署名すること３２０によって、ＧＯＰｎの内容が無傷である、すなわち改竄されていないことの検証をＧＯＰレベルで行うことができる。あるいは、ＧＯＰｎのフレームＩ、Ｐ１～Ｐ４のための１つまたは複数のフレームハッシュは、ＧＯＰｎのための連結されたＧＯＰハッシュを生成するためにＧＯＰｎのためのＧＯＰハッシュと連結されてもよく（図３ｂには図示せず）、次いで、連結されたＧＯＰハッシュは、署名付きＧＯＰハッシュを生成するためにデジタル署名によってデジタル署名される３２０。この代替形態では、ＧＯＰハッシュに関連する署名付きＧＯＰハッシュの部分を使用して、ＧＯＰの内容がＧＯＰレベルで無傷である、すなわち改竄されていないことを検証することができる。ＧＯＰが無傷ではないことが示された場合には、連結された１つまたは複数のフレームハッシュに関連する署名付きＧＯＰハッシュの一部は、デコーダ側でＧＯＰのフレームのコンテンツから生成されたフレームハッシュと比較することによって、１つまたは複数のフレームハッシュのどのフレームが改竄されているかを識別するために使用され得る。

【００４５】

さらに、ＧＯＰの並べ替えおよび検出不能なカットの識別を可能にするために、後続のＧＯＰｉ＋１の最初のフレームＩのフレームハッシュを生成し、署名前にＧＯＰｉのＧＯＰハッシュに追加することもできる。あるいは、ＧＯＰｉのＧＯＰハッシュは、ＧＯＰｉのフレームのフレームハッシュと後続のＧＯＰｉ＋１の最初のフレームＩのフレームハッシュとの連結をハッシュすることによって生成されてもよい。

【００４６】

図４は、各ＧＯＰがヘッダおよび１つまたは複数のフレームを含む、１つまたは複数のピクチャグループＧＯＰを含むビデオセグメントに署名するための本開示の装置４００の実施形態に関する概略図を示す。装置４００は、例えば監視カメラまたは身体装着カメラなどのカメラであってもよい。装置４００は回路４１０を含む。回路４１０は、装置４００の機能４３２，４３４，４３６，４３８を実行するように構成される。回路４１０は、中央処理装置（ＣＰＵ）、マイクロコントローラ、またはマイクロプロセッサなどのプロセッサ４１２を含むことができる。プロセッサ４１２は、プログラムコードを実行するように構成される。プログラムコードは、例えば、装置４００の機能４３２，４３４，４３６，４３８を実行するように構成されてもよい。

【００４７】

装置４００は、メモリ４３０をさらに含むことができる。メモリ４３０は、バッファ、フラッシュメモリ、ハードドライブ、取り外し可能な媒体、揮発性メモリ、不揮発性メモリ、ランダムアクセスメモリ（ＲＡＭ）、または別の適切な装置のうちの１つまたは複数であってもよい。典型的な構成では、メモリ４３０は、長期データ記憶用の不揮発性メモリと、回路４１０用のシステムメモリとして機能する揮発性メモリとを含むことができる。メモリ４３０は、データバスを介して回路４１０とデータを交換することができる。メモリ４３０と回路４１０との間に付随する制御線およびアドレスバスも存在してもよい。

【００４８】

装置４００の機能４３２，４３４，４３６，４３８は、装置４００の非一時的コンピュータ可読媒体（メモリ）４３０に記憶され、例えば回路４１０内のプロセッサ４１２を使用して回路４１０によって実行される実行可能論理ルーチン（例えば、コード行、ソフトウェアプログラムなど）の形態で具現化されてもよい。さらに、装置４００の機能４３２

，４３４，４３６，４３８は、スタンドアロンのソフトウェアアプリケーションであってもよく、またはソフトウェアアプリケーションの一部を形成してもよい。記載された機能は、処理ユニット、例えば回路４１０のプロセッサ４１２が実行するように構成された方法と考えることができる。また、記載された機能４３２，４３４，４３６，４３８はソフトウェアで実装されてもよいが、そのような機能は、専用のハードウェアもしくはファームウェア、またはハードウェア、ファームウェアおよび／もしくはソフトウェアの何らかの組み合わせを介して実行されてもよい。

【００４９】

回路４１０は、１つまたは複数のＧＯＰのうちのＧＯＰの各ＧＯＰについてＧＯＰハッシュを生成するように構成されたＧＯＰハッシュ生成機能を実行するように構成される。

【００５０】

回路４１０は、１つまたは複数のＧＯＰのうちのＧＯＰの各ＧＯＰについてＧＯＰハッシュにデジタル署名するように構成されたＧＯＰハッシュ署名機能を実行し、それによって１つまたは複数のＧＯＰのうちのＧＯＰの各ＧＯＰについてそれぞれの署名付きＧＯＰハッシュを生成するようにさらに構成される。

【００５１】

回路４１０は、ビデオセグメントに対し、１つまたは複数のＧＯＰの最後のＧＯＰの後に追加のＧＯＰを追加するように構成されたＧＯＰ追加機能を実行するようにさらに構成され、追加のＧＯＰはヘッダおよび１つまたは複数のフレームを含む。

【００５２】

回路４１０は、１つまたは複数のＧＯＰの各ＧＯＰについて、それぞれの署名付きＧＯＰハッシュを後続のＧＯＰのヘッダに保存するように構成された署名付きＧＯＰハッシュ保存機能を実行するようにさらに構成され、１つまたは複数のＧＯＰの最後のＧＯＰの署名付きＧＯＰハッシュは追加のＧＯＰのヘッダに保存される。

【００５３】

回路４１０によって実行される装置４００および機能４３２，４３４，４３６，４３８は、それぞれ図１、図２、図３ａおよび図３ｂに関連して説明した方法２００および方法２００の対応するステップとしてさらに適合させることができる。

【００５４】

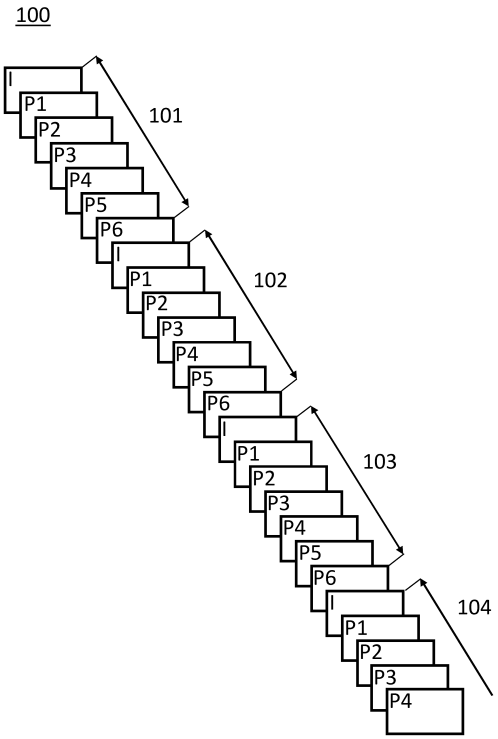
装置４００は、追加のＧＯＰの１つまたは複数のフレームを含むビデオセグメントのＧＯＰのフレームを符号化するためのエンコーダ（図示せず）をさらに含むことができる。

【００５５】

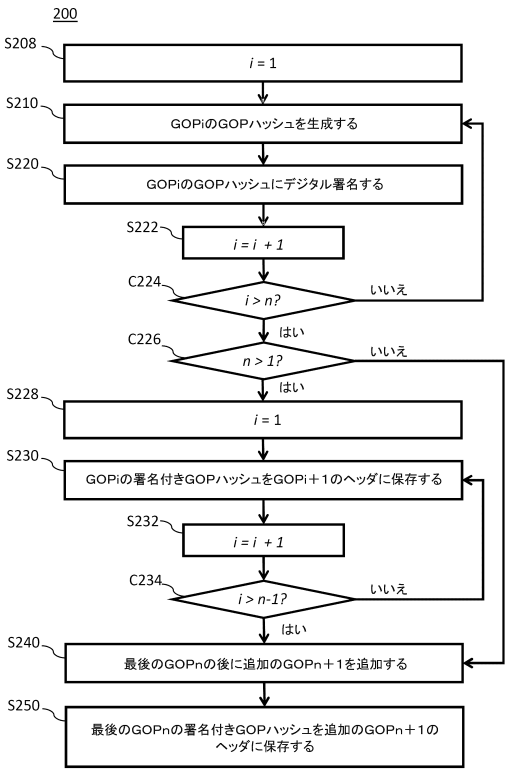
当業者であれば、本発明が上記の実施形態に限定されないことを理解する。それどころか、添付の特許請求の範囲内で多くの修正および変形が可能である。そのような修正および変形は、図面、開示、および添付の特許請求の範囲の研究から、特許請求される発明を実施する当業者によって理解および達成され得る。

【図面】

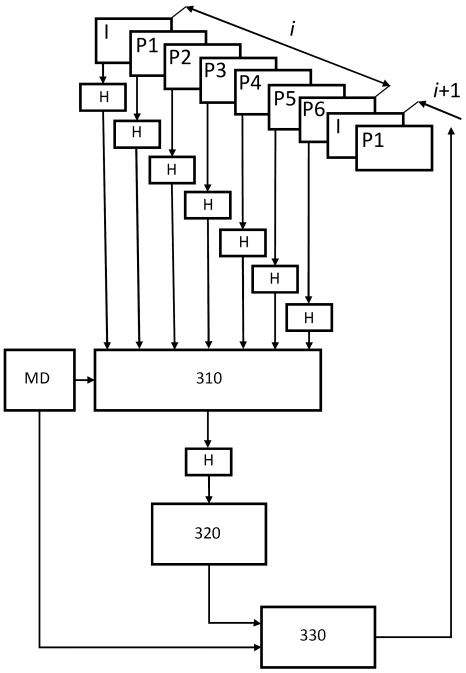
【図１】



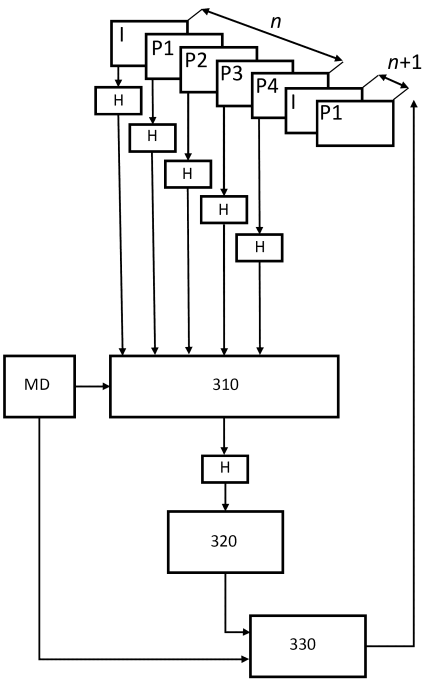
【図２】



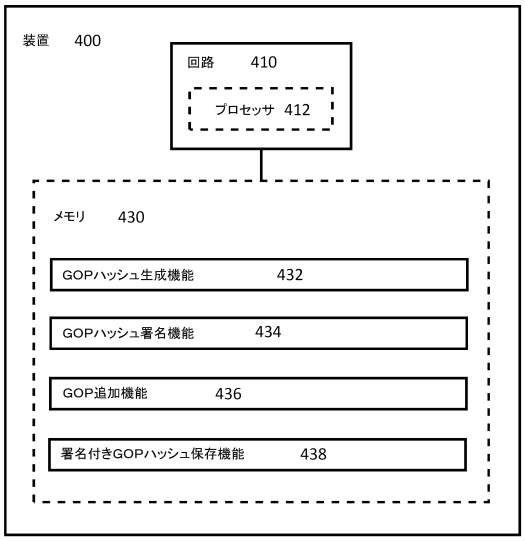
【図３ａ】



【図３ｂ】



【図４】


装置 400
回路 410
プロセッサ 412
メモリ 430
GOPハッシュ生成機能 432
GOPハッシュ署名機能 434
GOP追加機能 436
署名付きGOPハッシュ保存機能 438

フロントページの続き

(56)参考文献 特開２０１９－２０５１４０（ＪＰ，Ａ）
特開２００９－０８１５６４（ＪＰ，Ａ）
特開２００９－２００５９５（ＪＰ，Ａ）
国際公開第２００９／１０４２８４（WO，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｇ０６Ｆ　２１／６４
Ｈ０４Ｎ　７／１６７