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

特許第6353910号
(P6353910)

(45)発行日　平成30年7月4日(2018.7.4)　(24)登録日　平成30年6月15日(2018.6.15)

(51)Int.Cl.		F I		
G06T 7/00	(2017.01)	G06T	7/00	510D
H04L 9/32	(2006.01)	H04L	9/00	673D
G06T 1/00	(2006.01)	G06T	1/00	340A
G06F 21/32	(2013.01)	G06F	21/32	
G06F 21/60	(2013.01)	G06F	21/60	320

請求項の数 28　(全 33 頁)

(21)出願番号	特願2016-542869 (P2016-542869)
(86)(22)出願日	平成26年9月16日 (2014.9.16)
(65)公表番号	特表2016-538661 (P2016-538661A)
(43)公表日	平成28年12月8日 (2016.12.8)
(86)国際出願番号	PCT/US2014/055826
(87)国際公開番号	WO2015/039084
(87)国際公開日	平成27年3月19日 (2015.3.19)
審査請求日	平成29年8月30日 (2017.8.30)
(31)優先権主張番号	61/878,588
(32)優先日	平成25年9月16日 (2013.9.16)
(33)優先権主張国	米国(US)
(31)優先権主張番号	61/902,911
(32)優先日	平成25年11月12日 (2013.11.12)
(33)優先権主張国	米国(US)

(73)特許権者　516076717
アイベリファイ　インコーポレイテッド
アメリカ合衆国　ミズーリ　６４１０８，カンザス　シティ，　メイン　ストリート　１７４０，　スイート　１００
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100113413
弁理士　森下　夏樹
(74)代理人　100181674
弁理士　飯田　貴敏
(74)代理人　100181641
弁理士　石川　大輔
(74)代理人　230113332
弁護士　山本　健策

最終頁に続く

(54)【発明の名称】バイオメトリックテンプレートセキュリティおよびキー生成

(57)【特許請求の範囲】

【請求項１】

コンピュータ実装方法であって、

１つ以上の画像を受信することと、

前記受信された画像に基づいて、複数の着目点を識別することであって、各着目点は、複数の近傍タイルのうちのそれぞれのタイルに位置する、ことと、

前記複数の着目点に基づいて、複数の難読化データ点を生成することであって、前記複数の難読化データ点は、前記複数の着目点の空間分布および前記複数の難読化データ点の空間分布がタイルの各々内において実質的に類似するように、生成される、ことと、

前記複数の着目点および前記複数の難読化データ点に基づいて、難読化されたテンプレートを作成することと、

前記難読化されたテンプレートを記憶することと

を含む、方法。

【請求項２】

前記難読化されたテンプレート内のどの点が前記着目点であるかの記録を破棄することをさらに含む、請求項１に記載の方法。

【請求項３】

前記複数の難読化データ点および前記複数の着目点のうちの少なくとも一方の部分集合を使用して、キーをエンコードすることをさらに含む、請求項１に記載の方法。

【請求項４】

前記部分集合内の各点は、前記複数の着目点のうちの異なる１つに基づいて、決定される、請求項３に記載の方法。
【請求項５】
前記画像は、バイオメトリック像を備えている、請求項１に記載の方法。
【請求項６】
前記画像は、眼の領域の画像を備え、各眼領域画像は、それぞれの眼領域の血管系のビューを備え、前記着目点は、血管の着目点を備えている、請求項５に記載の方法。
【請求項７】
１つ以上の実記述子を各着目点に関連付けることをさらに含み、各実記述子は、対応する着目点を包囲する１つ以上の局所を記述する、請求項１に記載の方法。
【請求項８】
１つ以上の合成記述子を各難読化データ点に関連付けることをさらに含み、各合成記述子は、前記実記述子との統計的類似性を備えている、請求項７に記載の方法。
【請求項９】
１つ以上の第２の画像を受信することと、
前記受信された第２の画像に基づいて、第２の複数の着目点を識別することと、
前記第２の複数の着目点に基づいて、確認テンプレートを作成することと、
前記確認テンプレートと前記難読化されたテンプレートとを比較することにより、複数の一致している着目点を識別することと、
前記複数の一致している着目点に基づいて、ユーザを認証することと
をさらに含む、請求項８に記載の方法。
【請求項１０】
前記比較することは、前記実記述子および前記合成記述子のうちの１つ以上に基づいて、前記複数の一致している着目点を識別することを含む、請求項９に記載の方法。
【請求項１１】
前記実記述子および前記合成記述子の次元性を低減させることをさらに含む、請求項９に記載の方法。
【請求項１２】
前記比較することは、次元性を低減させられた１つ以上の記述子に基づいて、前記複数の一致している着目点を識別することを含む、請求項１１に記載の方法。
【請求項１３】
前記実記述子および前記合成記述子を等長でスクランブリングすることをさらに含む、請求項９に記載の方法。
【請求項１４】
前記比較することは、前記スクランブリングされた記述子のうちの１つ以上に基づいて、前記複数の一致している着目点を識別することを含む、請求項１３に記載の方法。
【請求項１５】
前記複数の一致している着目点の少なくとも部分集合に基づいて、キーをデコードすることをさらに含む、請求項９に記載の方法。
【請求項１６】
１つ以上のコンピュータを備えているシステムであって、前記１つ以上のコンピュータは、
１つ以上の画像を受信することと、
前記受信された画像に基づいて、複数の着目点を識別することであって、各着目点は、複数の近傍タイルのうちのそれぞれのタイルに位置する、ことと、
前記複数の着目点に基づいて、複数の難読化データ点を生成することであって、前記複数の難読化データ点は、前記複数の着目点の空間分布および前記複数の難読化データ点の空間分布がタイルの各々内において実質的に類似するように、生成される、ことと、
前記複数の着目点および前記複数の難読化データ点に基づいて、難読化されたテンプレートを作成することと、

前記難読化されたテンプレートを記憶することと
を含む動作を行うようにプログラムされている、システム。
【請求項１７】
前記動作は、前記難読化されたテンプレート内のどの点が前記着目点であるかの記録を破棄することをさらに含む、請求項１６に記載のシステム。
【請求項１８】
前記動作は、前記複数の難読化データ点および前記複数の着目点のうちの少なくとも一方の部分集合を使用して、キーをエンコードすることをさらに含む、請求項１６に記載のシステム。
【請求項１９】
前記部分集合内の各点は、前記複数の着目点のうちの異なる１つに基づいて、決定される、請求項１８に記載のシステム。
【請求項２０】
前記画像は、バイオメトリック像を備えている、請求項１６に記載のシステム。
【請求項２１】
前記画像は、眼の領域の画像を備え、各眼領域画像は、それぞれの眼領域の血管系のビューを備え、前記着目点は、血管の着目点を備えている、請求項２０に記載のシステム。
【請求項２２】
前記動作は、１つ以上の実記述子を各着目点に関連付けることをさらに含み、各実記述子は、対応する着目点を包囲する１つ以上の局所を記述する、請求項１６に記載のシステム。
【請求項２３】
前記動作は、１つ以上の合成記述子を各難読化データ点に関連付けることをさらに含み、各合成記述子は、前記実記述子との統計的類似性を備えている、請求項２２に記載のシステム。
【請求項２４】
前記動作は、
１つ以上の第２の画像を受信することと、
前記受信された第２の画像に基づいて、第２の複数の着目点を識別することと、
前記第２の複数の着目点に基づいて、確認テンプレートを作成することと、
前記確認テンプレートと前記難読化されたテンプレートとを比較することにより、複数の一致している着目点を識別することと、
前記複数の一致している着目点に基づいて、ユーザを認証することと
をさらに含む、請求項２３に記載のシステム。
【請求項２５】
前記比較することは、前記実記述子および前記合成記述子のうちの１つ以上に基づいて、前記複数の一致している着目点を識別することを含む、請求項２４に記載のシステム。
【請求項２６】
前記動作は、前記実記述子および前記合成記述子の次元性を低減させることをさらに含み、前記比較することは、次元性を低減させられた１つ以上の記述子に基づいて、前記複数の一致している着目点を識別することを含む、請求項２４に記載のシステム。
【請求項２７】
前記動作は、前記実記述子および前記合成記述子を等長でスクランブリングすることをさらに含み、前記比較することは、前記スクランブリングされた記述子のうちの１つ以上に基づいて、前記複数の一致している着目点を識別することを含む、請求項２４に記載のシステム。
【請求項２８】
前記動作は、前記複数の一致している着目点の少なくとも部分集合に基づいて、キーをデコードすることをさらに含む、請求項２４に記載のシステム。
【発明の詳細な説明】

【技術分野】
【０００１】
（関連出願の引用）
本願は、米国特許出願第１４／４５４，１４８号（２０１４年８月７日出願、名称「Ｂｉｏｍｅｔｒｉｃ Ｔｅｍｐｌａｔｅ Ｓｅｃｕｒｉｔｙ ａｎｄ Ｋｅｙ Ｇｅｎｅｒａｔｉｏｎ」）に基づく優先権および利益を主張し、該特許出願は、米国仮特許出願第６１／８７８，５８８号（２０１３年９月１６日出願、名称「Ｉｍａｇｅ Ｄｅｔｅｃｔｉｏｎ，Ａｕｔｈｅｎｔｉｃａｔｉｏｎ，ａｎｄ Ｉｎｆｏｒｍａｔｉｏｎ Ｈｉｄｉｎｇ」）、米国仮特許出願第６１／９０２，９１１号（２０１３年１１月１２日出願、名称「Ｄｅｔｅｃｔｉｏｎ，Ａｕｔｈｅｎｔｉｃａｔｉｏｎ，ａｎｄ Ｉｎｆｏｒｍａｔｉｏｎ Ｈｉｄｉｎｇ」）に基づく優先権および利益を主張する。上記出願の全体は、参照により本明細書に引用される。
【０００２】
本開示は、概して、バイオメトリック認証に関し、より具体的には、バイオメトリックテンプレートをセキュア化し、バイオメトリックテンプレートを使用して、キーをエンコードおよびデコードするためのシステムおよび方法に関する。
【背景技術】
【０００３】
多くの場合、所有物またはリソースへのアクセスを特定の個人に制限することが、望ましい。バイオメトリックシステムは、個人の識別を認証し、リソースへのアクセスの許可または拒否のいずれかを行うために使用されることができる。例えば、虹彩スキャナが、バイオメトリックセキュリティシステムによって使用され、個人の虹彩内の独特の構造に基づいて、個人を識別することができる。登録プロセスの際等に個人から捕捉されるバイオメトリックデータは、後に個人の識別を確認するために使用される、テンプレートとして記憶されることができる。テンプレートは、例えば、認証サーバ上に遠隔で、またはカメラを伴う携帯電話等、バイオメトリック読み取り値を捕捉する能力を有するデバイス上にローカルに記憶されることができる。しかしながら、テンプレートをそのオリジナル形態またはそこからオリジナルテンプレートが導出され得る形態に維持することは、テンプレートのセキュリティが損なわれるであろうリスクをもたらす。
【発明の概要】
【課題を解決するための手段】
【０００４】
バイオメトリックテンプレートをセキュア化し、バイオメトリックテンプレートを使用して、キーをエンコードおよびデコードするためのシステムおよび方法が、開示される。一側面では、コンピュータ実装方法は、１つ以上の画像を受信することと、受信された画像に基づいて、複数の着目点を識別することと、着目点に基づいて、複数の難読化データ点を生成することと、着目点および難読化データ点に基づいて、難読化されたテンプレートを生成することと、難読化されたテンプレートを記憶することとを含む。本側面の他の実施形態は、対応するシステムおよびコンピュータプログラムを含む。
【０００５】
一実装では、難読化データ点は、着目点の空間分布および難読化データ点の空間分布が実質的に類似するように、生成される。
【０００６】
別の実装では、本方法はさらに、１つ以上の実記述子を各着目点に関連付けることを含み、各実記述子は、対応する着目点を包囲する１つ以上の局所を記述する。
【０００７】
さらなる実装では、本方法はさらに、難読化されたテンプレート内のどの点が着目点であるかの記録を破棄することを含む。
【０００８】
さらに別の実装では、本方法はさらに、難読化データ点および着目点のうちの少なくと

も１つの部分集合を使用して、キーをエンコードすることを含む。部分集合内の各点は、着目点のうちの異なる１つに基づいて、決定されることができる。

【０００９】

別の実装では、画像は、バイオメトリック像を備えている。画像は、眼の領域の画像を備えていることができ、各眼領域画像は、それぞれの眼領域の血管系のビューを備えている。着目点は、血管の着目点を備えていることができる。

【００１０】

一実装では、本方法はさらに、１つ以上の合成記述子を各難読化データ点に関連付けることを含み、各合成記述子は、実記述子との統計的類似性を備えている。

【００１１】

別の実装では、本方法はさらに、１つ以上の第２の画像を受信することと、受信された第２の画像に基づいて、第２の複数の着目点を識別することと、第２の複数の着目点に基づいて、確認テンプレートを作成することと、確認テンプレートと難読化されたバイオメトリックテンプレートを比較し、複数の一致している着目点を識別することと、一致している着目点に基づいて、ユーザを認証することとを含む。比較することは、実記述子および合成記述子のうちの１つ以上に基づいて、一致している着目点を識別することを含むことができる。

【００１２】

さらなる実装では、本方法はさらに、実記述子および合成記述子の次元性を低減させることを含む。比較することは、次元性が低減された記述子のうちの１つ以上に基づいて、一致している着目点を識別することを含むことができる。

【００１３】

さらなる実装では、本方法はさらに、実記述子および合成記述子を等長でスクランブリングすることを含む。比較することはさらに、スクランブリングされた記述子の１つ以上に基づいて、一致している着目点を識別することを含むことができる。

【００１４】

さらに別の実装では、本方法はさらに、一致している着目点の少なくとも部分集合に基づいて、キーをデコードすることを含む。

【００１５】

本明細書に説明される主題の１つ以上の実装の詳細は、付随の図面および以下の説明に記載される。本主題の他の特徴、側面、および利点は、説明、図面、および請求項から明白となるであろう。

本願明細書は、例えば、以下の項目も提供する。

（項目１）

コンピュータ実装方法であって、

１つ以上の画像を受信することと、

前記受信された画像に基づいて、複数の着目点を識別することと、

前記着目点に基づいて、複数の難読化データ点を生成することと、

前記着目点および前記難読化データ点に基づいて、難読化されたテンプレートを生成することと、

前記難読化されたテンプレートを記憶することと

を含む、方法。

（項目２）

前記難読化データ点は、前記着目点の空間分布および前記難読化データ点の空間分布が実質的に類似するように、生成される、項目１に記載の方法。

（項目３）

前記難読化されたテンプレート内のどの点が前記着目点であるかの記録を破棄することをさらに含む、項目１に記載の方法。

（項目４）

前記難読化データ点および前記着目点のうちの少なくとも１つの部分集合を使用して、

キーをエンコードすることをさらに含む、項目１に記載の方法。
（項目５）
前記部分集合内の各点は、前記着目点のうちの異なる１つに基づいて、決定される、項目４に記載の方法。
（項目６）
前記画像は、バイオメトリック像を備えている、項目１に記載の方法。
（項目７）
前記画像は、眼の領域の画像を備え、各眼領域画像は、それぞれの眼領域の血管系のビューを備え、前記着目点は、血管の着目点を備えている、項目６に記載の方法。
（項目８）
１つ以上の実記述子を各着目点に関連付けることをさらに含み、各実記述子は、対応する着目点を包囲する１つ以上の局所を記述する、項目１に記載の方法。
（項目９）
１つ以上の合成記述子を各難読化データ点に関連付けることをさらに含み、各合成記述子は、前記実記述子との統計的類似性を備えている、項目８に記載の方法。
（項目１０）
１つ以上の第２の画像を受信することと、
前記受信された第２の画像に基づいて、第２の複数の着目点を識別することと、
前記第２の複数の着目点に基づいて、確認テンプレートを作成することと、
前記確認テンプレートを前記難読化されたテンプレートと比較し、複数の一致している着目点を識別することと、
前記一致している着目点に基づいて、ユーザを認証することと
をさらに含む、項目９に記載の方法。
（項目１１）
前記比較することは、前記実記述子および合成記述子のうちの１つ以上に基づいて、前記一致している着目点を識別することを含む、項目１０に記載の方法。
（項目１２）
前記実記述子および前記合成記述子の次元性を低減させることをさらに含む、項目１０に記載の方法。
（項目１３）
前記比較することは、前記次元性低減記述子のうちの１つ以上に基づいて、前記一致している着目点を識別することを含む、項目１２に記載の方法。
（項目１４）
前記実記述子および前記合成記述子を等長でスクランブリングすることをさらに含む、項目１０に記載の方法。
（項目１５）
前記比較することは、前記スクランブリングされた記述子のうちの１つ以上に基づいて、前記一致している着目点を識別することを含む、項目１４に記載の方法。
（項目１６）
前記一致している着目点の少なくとも部分集合に基づいて、キーをデコードすることをさらに含む、項目１０に記載の方法。
（項目１７）
１つ以上のコンピュータを備えているシステムであって、前記コンピュータは、
１つ以上の画像を受信することと、
前記受信された画像に基づいて、複数の着目点を識別することと、
前記着目点に基づいて、複数の難読化データ点を生成することと、
前記着目点および前記難読化データ点に基づいて、難読化されたテンプレートを生成することと、
前記難読化されたテンプレートを記憶することと
を含む動作を行うようにプログラムされている、システム。

（項目１８）
前記難読化データ点は、前記着目点の空間分布および前記難読化データ点の空間分布が実質的に類似するように、生成されている、項目１７に記載のシステム。
（項目１９）
前記動作は、前記難読化されたテンプレート内のどの点が前記着目点であるかの記録を破棄することをさらに含む、項目１７に記載のシステム。
（項目２０）
前記動作は、前記難読化データ点および前記着目点のうちの少なくとも１つの部分集合を使用して、キーをエンコードすることをさらに含む、項目１７に記載のシステム。
（項目２１）
前記部分集合内の各点は、前記着目点のうちの異なる１つに基づいて、決定されている、項目２０に記載のシステム。
（項目２２）
前記画像は、バイオメトリック像を備えている、項目１７に記載のシステム。
（項目２３）
前記画像は、眼の領域の画像を備え、各眼領域画像は、前記それぞれの眼領域の血管系のビューを備え、前記着目点は、血管の着目点を備えている、項目２２に記載のシステム。
（項目２４）
前記動作は、１つ以上の実記述子を各着目点に関連付けることをさらに含み、各実記述子は、対応する着目点を包囲する１つ以上の局所を記述する、項目１７に記載のシステム。
（項目２５）
前記動作は、１つ以上の合成記述子を各難読化データ点に関連付けることをさらに含み、各合成記述子は、前記実記述子との統計的類似性を備えている、項目２４に記載のシステム。
（項目２６）
前記動作は、
１つ以上の第２の画像を受信することと、
前記受信された第２の画像に基づいて、第２の複数の着目点を識別することと、
前記第２の複数の着目点に基づいて、確認テンプレートを作成することと、
前記確認テンプレートを前記難読化されたテンプレートと比較し、複数の一致している着目点を識別することと、
前記一致している着目点に基づいて、ユーザを認証することと
をさらに含む、項目２５に記載のシステム。
（項目２７）
前記比較することは、前記実記述子および合成記述子のうちの１つ以上に基づいて、前記一致している着目点を識別することを含む、項目２６に記載のシステム。
（項目２８）
前記動作は、前記実記述子および前記合成記述子の次元性を低減させることをさらに含み、前記比較することは、前記次元性低減記述子のうちの１つ以上に基づいて、前記一致している着目点を識別することを含む、項目２６に記載のシステム。
（項目２９）
前記動作は、前記実記述子および前記合成記述子を等長でスクランブリングすることをさらに含み、前記比較することは、前記スクランブリングされた記述子のうちの１つ以上に基づいて、前記一致している着目点を識別することを含む、項目２６に記載のシステム。
（項目３０）
前記動作は、前記一致している着目点の少なくとも部分集合に基づいて、キーをデコードすることをさらに含む、項目２６に記載のシステム。

【００１６】
図面中、同様の参照文字は、概して、異なる図全体を通して、同一部分を指す。また、図面は、必ずしも、正確な縮尺ではなく、代わりに、概して実装の原理の例証に強調が置かれる。以下の説明では、種々の実装は、以下の図面を参照して説明される。
【図面の簡単な説明】
【００１７】
【図１】図１は、ある実装による、バイオメトリックテンプレートセキュリティおよびキー生成のためのシステムの略図を描写する。
【図２】図２は、ある実装による、バイオメトリックテンプレートをセキュア化し、秘密キーをエンコード／デコードする方法を描写する。
【図３】図３は、例示的血管の着目点を伴う、眼内画像を描写する。
【図４Ａ】図４Ａは、埋め込まれた難読化データ点を伴う、図３の血管の着目点を描写する。
【図４Ｂ】図４Ｂは、図３の眼画像上に重ねられた図４Ｂからの難読化されたデータ点を描写する。
【図５】図５は、タグ付けされた点の部分集合を伴う、図４Ａの血管の着目点および難読化データ点を描写する。
【発明を実施するための形態】
【００１８】
白眼内の個人の可視血管系の固有の特徴は、個人を識別または認証するために使用されることができる。例えば、ユーザの白眼の画像が、ユーザを認証し、リソースへのユーザアクセスを許可または拒否するために、取得および分析され、眼の特徴をバイオメトリックテンプレートと比較することができる。白眼内の血管の撮像およびパターンマッチングならびに特徴抽出およびマッチングのための解決策の実装は、２０１３年２月５日発行の米国特許第８，３６９，５９５号「Ｔｅｘｔｕｒｅ Ｆｅａｔｕｒｅｓ ｆｏｒ Ｂｉｏｍｅｔｒｉｃ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ」、および２０１４年５月９日出願の米国特許出願第１４／２７４，３８５号「Ｆｅａｔｕｒｅ Ｅｘｔｒａｃｔｉｏｎ ａｎｄ Ｍａｔｃｈｉｎｇ ｆｏｒ Ｂｉｏｍｅｔｒｉｃ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ」に説明され、その全体は、参照することによって本明細書に組み込まれる。
【００１９】
例えば、個人の可視血管系の独特の構造は、個人の白眼の画像のテクスチャ特徴に反映されることができる。画像は、テクスチャ分析のための白眼上の領域を識別するためにセグメント化されることができ、これらの領域内の個人血管系のテクスチャ特徴の記述子を決定するために、一組のフィルタが適用されることができる。フィルタ出力から導出される記述子のベクトルは、記述子ベクトルに組み立てられることができる。次いで、認証または識別動作中に、ユーザに対して決定される記述子ベクトルは、ユーザと登録された個人との間の一致の可能性を決定するために、登録された個人に対して記憶されたバイオメトリック記録からの対応する記述子ベクトルと比較されることができる。
【００２０】
本明細書に説明されるテンプレートセキュリティおよびキー生成技法の種々の実装は、多数または十分な数の「チャフ」、すなわち、判別不能雑音要素を使用する、バイオメトリックテンプレートのステガノグラフィ難読化に基づく。デバイス特定のスクランブリング空間内における確認成功に応じて識別されるチャフ要素の部分集合が、エンコードされた秘密をもたらす方程式系を解くために利用される。これらのトークンは、高エントロピかつ取り消し可能であり、ユーザの生物学的特徴に関して何も明らかにしない。
【００２１】
図１は、セキュアなバイオメトリックテンプレートを生成し、ユーザ確認を行い、バイオメトリックテンプレートに基づいて、秘密キーをエンコードおよびデコードするための局所的なシステムの一実装を図示する。ユーザデバイス１００は、画像センサ１３０と、プロセッサ１４０と、メモリ１５０と、バイオメトリックハードウェアおよび／またはソ

フトウェア１６０と、システムバスとを含むことができ、システムバスは、メモリ１５０を含む種々のシステム構成要素をプロセッサ１４０に連結する。ユーザデバイス１００は、限定ではないが、スマートフォン、スマートウォッチ、スマートグラス、タブレットコンピュータ、ポータブルコンピュータ、テレビ、ゲームデバイス、音楽プレーヤ、携帯電話、ラップトップ、パームトップ、スマートまたはダム端末、ネットワークコンピュータ、携帯情報端末、ワイヤレスデバイス、情報機器、ワークステーション、ミニコンピュータ、メインフレームコンピュータ、または本明細書に説明される機能性を実行することができる、汎用コンピュータもしくは特殊目的ハードウェアデバイスとして動作させられる他のコンピューティングデバイスを含むことができる。

【００２２】

バイオメトリックハードウェアおよび／またはソフトウェア１６０は、画像センサ１３０による画像捕捉に関する動作を行うための画像処理モジュール１６２を含む。例えば、画像処理モジュール１６２は、ユーザ１１０の眼の画像に対してセグメント化および強調を行い、血管構造の分離を補助することができる。テンプレートセキュリティモジュール１６６は、血管系像に基づいて、バイオメトリックテンプレートを作成し、本明細書に説明されるように、テンプレートに対して種々の難読化およびスクランブリング動作を行い、有用性を維持しながら、テンプレートセキュリティを増加させる。確認モジュール１７４は、バイオメトリック読み取り値の捕捉に応じて形成されたバイオメトリック確認テンプレートと以前に記憶された登録テンプレートとの間でマッチング動作を行うことによって、ユーザ１１０の識別を検証する。キーモジュール１７８は、バイオメトリック登録テンプレートに基づいて、ユーザ１１０のための秘密キーをエンコードし、確認テンプレートを使用して、ユーザの識別の確認成功に応じて、キーをデコードすることができる。

【００２３】

本明細書に説明されるシステムの実装は、適切なハードウェアまたはソフトウェアを使用することができる。例えば、システムは、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステム、Ａｐｐｌｅ　ＯＳ　Ｘ（登録商標）オペレーティングシステム、Ａｐｐｌｅ　ｉＯＳ（登録商標）プラットフォーム、Ｇｏｏｇｌｅ　Ａｎｄｒｏｉｄ™プラットフォーム、Ｌｉｎｕｘ（登録商標）オペレーティングシステム、およびＵＮＩＸ（登録商標）オペレーティングシステムの他のバリアント等のオペレーティングシステムを起動可能なソフトウェア上で実行することができる。システムは、メモリ１５０内に記憶され、プロセッサ１４０上で実行される複数のソフトウェア処理モジュール（例えば、画像処理モジュール１６２、テンプレートセキュリティモジュール１６６、確認モジュール１７４、およびキーモジュール１７８）を含むことができる。例証として、プログラムモジュールは、機械言語またはオブジェクトコードに変換され、プロセッサまたはプロセッサが命令を実行することを可能にする、１つ以上の好適なプログラミング言語の形態であることができる。ソフトウェアは、好適なプログラミング言語またはフレームワークで実装される、スタンドアロンアプリケーションの形態であることができる。

【００２４】

加えて、または代替として、機能性の一部または全部は、遠隔で、クラウド内で、またはサービスとしてのソフトウェア（ｓｏｆｔｗａｒｅ－ａｓ－ａ－ｓｅｒｖｉｃｅ）を介して、行われることができる。例えば、ある機能（例えば、画像処理、テンプレート作成、テンプレートマッチング等）は、１つ以上の遠隔サーバまたはユーザデバイスと通信する他のデバイス上で行われることができる。遠隔機能性は、十分なメモリ、データ記憶、および処理能力を有し、サーバクラスオペレーティングシステム（例えば、Ｏｒａｃｌｅ（登録商標）Ｓｏｌａｒｉｓ（登録商標）、ＧＮＵ／Ｌｉｎｕｘ（登録商標）、およびＭｉｃｒｏｓｏｆｔ（登録商標）Ｗｉｎｄｏｗｓ（登録商標）系のオペレーティングシステム）を起動させる、サーバクラスコンピュータ上で実行することができる。サーバとユーザデバイスとの間の通信は、例えば、標準的電話回線、ＬＡＮまたはＷＡＮリンク（例えば、Ｔ１、Ｔ３、５６ｋｂ、Ｘ．２５）、ブロードバンド接続（ＩＳＤＮ、フレームリレー、ＡＴＭ）、ワイヤレスリンク（８０２．１１（Ｗｉ－Ｆｉ）、Ｂｌｕｅｔｏｏｔｈ（

登録商標）、ＧＳＭ（登録商標）、ＣＤＭＡ等）等の媒体を経由して生じることができる。他の通信媒体も考えられる。ネットワークは、ＴＣＰ／ＩＰプロトコル通信およびウェブブラウザによって行われるＨＴＴＰ／ＨＴＴＰＳ要求を伝えることができ、ユーザデバイスとサーバとの間の接続は、そのようなＴＣＰ／ＩＰネットワークを経由して通信されることができる。他の通信プロトコルも、考えられる。

【００２５】

本明細書に説明される技法の方法ステップは、入力データに基づいて動作することによって、１つ以上のコンピュータプログラムを実行し、機能を果たし、出力を生成する１つ以上のプログラマブルプロセッサによって行われることができる。方法ステップはまた、特殊目的論理回路、例えば、ＦＰＧＡ（フィールドプログラマブルゲートアレイ）またはＡＳＩＣ（特定用途向け集積回路）によって行われることができ、モジュールは、そのようなものとして実装されることができる。モジュールは、コンピュータプログラムおよび／またはその機能性を実装するプロセッサ／特殊回路の一部を指すことができる。

【００２６】

コンピュータプログラムの実行のために好適なプロセッサは、一例として、汎用および特殊目的マイクロプロセッサの両方を含む。概して、プロセッサは、読み取り専用メモリまたはランダムアクセスメモリまたは両方から命令およびデータを受信するであろう。コンピュータの必須要素は、命令を実行するためのプロセッサと、命令およびデータを記憶するための１つ以上のメモリデバイスである。コンピュータプログラム命令およびデータを具現化するために好適な情報担体は、一例として、半導体メモリデバイス、例えば、ＥＰＲＯＭ、ＥＥＰＲＯＭ、およびフラッシュメモリデバイス、磁気ディスク、例えば、内部ハードディスクまたは取り外し可能なディスク、光磁気ディスク、ならびにＣＤ－ＲＯＭおよびＤＶＤ－ＲＯＭディスクを含む、あらゆる形態の不揮発性メモリを含む。１つ以上のメモリは、プロセッサによって実行されると、モジュールおよび本明細書に説明される他の構成要素を形成し、構成要素に関連付けられた機能性を果たす命令を記憶することができる。プロセッサおよびメモリは、特殊目的論理回路によって補完されるか、またはその中に組み込まれることができる。

【００２７】

システムはまた、分散型コンピューティング環境において実践されることができ、タスクは、通信ネットワークを通してリンクされる遠隔処理デバイスによって行われる。分散型コンピューティング環境では、プログラムモジュールは、メモリ記憶デバイスを含む、ローカルおよび遠隔両方のコンピュータ記憶媒体内に位置することができる。本明細書に説明されるもの以外のタイプのシステムハードウェアおよびソフトウェアもまた、デバイスの容量および要求されるデータ処理能力の量に応じて、使用されることができる。システムはまた、前述のもの等の仮想化されたオペレーティングシステムを実行し、本明細書に説明されるもの等のハードウェアを有する１つ以上のコンピュータ上で動作する、１つ以上の仮想機械上に実装されることができる。

【００２８】

また、システムおよび方法の実装は、１つ以上の製造品上もしくはその中に具現化される１つ以上のコンピュータ読み取り可能なプログラムとして提供されることができることに留意されたい。プログラム命令は、データ処理装置による実行のために好適な受信機装置への伝送のために、情報をエンコードするために生成される、人工的に生成される伝搬信号、例えば、機械生成電気、光学、または電磁信号上にエンコードされることができる。コンピュータ記憶媒体は、コンピュータ読み取り可能な記憶デバイス、コンピュータ読み取り可能な記憶基板、ランダムまたはシリアルアクセスメモリアレイもしくはデバイス、またはそれらのうちの１つ以上の組み合わせであるか、またはその中に含まれることができる。さらに、コンピュータ記憶媒体は、伝搬信号ではないが、コンピュータ記憶媒体は、人工的に生成される伝搬信号内にエンコードされるコンピュータプログラム命令の源またはその宛先であることができる。コンピュータ記憶媒体はまた、１つ以上の別個の物理的構成要素もしくは媒体（例えば、複数のＣＤ、ディスク、または他の記憶デバイス）

である、またはその中に含まれることができる。

【００２９】

図２を参照すると、一実装では、バイオメトリックテンプレートをセキュア化する方法が、ユーザの眼の画像、および／またはそれの１つ以上の領域を受信することによって開始する（ステップ２０２）。画像は、画像センサ１３０を有するデバイス１００、例えば、正面に面したカメラを伴う電話またはタブレットを使用して捕捉されることができる。複数の画像が受信される場合、単一画像が、バイオメトリック識別のためにその好適性に基づいて自動的に選択されることができるか、または、画像の一部もしくは全部が自動的に選択され、平均化されて単一の組み合わせ画像をもたらすことができる（ステップ２０６）。強膜、すなわち、白眼を含む画像領域は、画像処理モジュール１６２によって、セグメント化、鮮明化、コントラスト強調され、および／またはいくつかの青色－緑色層でフィルタ処理され、白眼内で可視の血管パターンの最適描写を提供する（ステップ２１２）。

【００３０】

ステップ２１８では、血管パターンの描写に基づいて、テンプレートセキュリティモジュール１６６が、血管の着目点を識別し、ステップ２２２において、モジュール１６６は、各局所において一連の画像記述子を対応する血管の着目点に関連付け、各着目点に対して、場所－記述子構造を作成する。この段階において、眼画像は、破棄されることができる（ステップ２２６）。結果として生じる組の血管の着目点とそれらの関連付けられた局所画像記述子は、基本バイオメトリックテンプレートを形成する（ステップ２３０）。テンプレートが、ユーザを登録するために意図されている場合、テンプレートは、以下に説明されるように、プライベートかつセキュアな様式においてデバイス１００上にローカルに保存されることができる（例えば、メモリ１５０内に）。

【００３１】

バイオメトリックテンプレートをセキュア化するために、テンプレートセキュリティモジュール１６６は、場所－記述子構造を、いくつかの生成された「チャフ」要素、すなわち、難読化データ点内に「秘匿」し、それらは、同様に構造化され、実際の血管の着目点と統計的に判別不能であり得る（ステップ２３４）。ステップ２４２において、チャフ対非チャフ（すなわち、真正血管の着目点）要素の全記録を破棄する前に、各血管の着目点は、チャフ点（または、別の血管の着目点）を「タグ」付けする（ステップ２３８）。具体的には、キーモジュール１７８が、血管の着目点をセキュアな一方向関数に入力し、タグ付けされるべきチャフ点（または、血管の着目点）を出力として指定する。これらのタグ付けされた点は、以下にさらに説明されるように、長いランダムなキーの線形投影を取り入れ、エンコードし（ステップ２５０）、かつユーザの識別の確認成功に応じてキーをデコードするキーモジュール１７８によって使用されることができる。

【００３２】

これらのチャフデリゲート型動作（ｃｈａｆｆ－ｄｅｌｉｇａｔｅｄ　ｏｐｅｒａｔｉｏｎ）はさらに、さらなるプライバシー、セキュリティ、および取り消し可能性のために、種々の機能性（サロゲートバイオメトリック確認およびキー生成等）を真正テンプレート要素から切り離す。テンプレートセキュリティモジュール１６６はさらに、ステップ２４６において、例えば、統計的脱相関および正規化、および／または、デバイス特定の等長ソルト付与（ｉｓｏｍｅｔｒｉｃ　ｓａｌｔｉｎｇ）および次元リシャッフリングにより、記述子をスクランブリングすることによって、チャフ難読化テンプレートをセキュア化し、それによって、特に、デバイス１００から伝送される場合、生物測定的に導出された情報があらわにされないことを確実にする。確認モジュール１７４は、この独特のデバイス特有かつスクランブリングされた空間における識別確認の間に、バイオメトリックテンプレートマッチングを行い、さらに別の層のセキュリティ、プライバシー、および取り消し可能性を局所的マッチングおよびキー生成ルーチンに追加することができる。ステップ２５４では、チャフで難読化され、スクランブリングされた記述子テンプレートは、デバイス上に局所的に記憶される（または、他の実装では、テンプレートは、遠隔で記憶さ

れる）。

【００３３】

ユーザの識別の確認の間、同一または類似の画像捕捉、セグメント化、および強調ステップが、画像処理モジュール１６２によって実施される。同様に、血管の着目点が、登録中に使用された独特のデバイスおよびソフトウェア特有シグネチャを使用して、テンプレートセキュリティモジュール１６６によって、見出され、その局所記述子が、計算され、次いで、スクランブリングされ（ステップ２５８）、それによって、確認テンプレートを作成する（ステップ２６２）。これは、登録および確認が同一デバイスおよびソフトウェアインスタンス上においてのみ生じ得ることを確実にする。ステップ２６６において、確認モジュール１７４によって、スクランブリングされた空間内で完了される、マッチングプロセスは、真正確認成功の場合、確認テンプレートを難読化されたテンプレートと比較することによって、最小数の真正血管の着目点を識別する。識別された真正血管の着目点は、順に、登録プロセスにおいて前もってタグ付けされた十分な大きさの情報担持チャフ点の部分集合をあらわにする（ステップ２６８）。この最小数の真正点、したがって、タグ付けされたチャフ点は、キーエンコード方程式系と同じ順序である。キーモジュール１７８は、次いで、タグ付けされたチャフ点からの情報を使用して、方程式系を解き、デコードされたキーを得ることができる（ステップ２７２）。一実装では、キーは、不変５１２ビット長であって、少なくとも６４ビットのエントロピを有する。

【００３４】

本明細書に提示される種々のシステムおよび方法は、バイオメトリック眼像および可視血管系から導出される着目点を利用するが、開示される技法の他の実装および用途も、検討されることを理解されたい。例えば、他の実装では、特徴および／または着目点は、指紋または顔スキャン等の他のバイオメトリック像データ内で識別される。類似の撮像処理手技が、像内の着目特徴／点を強調および分離するために行われることができ、特徴／点が識別されると、本明細書に説明されるものと同一または実質的に同様の難読化、スクランブリング、確認、および／またはキーエンコード／デコード技法が、適用されることができる。さらに、本明細書に提示される種々のシステムおよび方法は、バイオメトリック撮像および認証と併せて使用される必要はないことに留意されたい。むしろ、本明細書に開示される技法は、他のタイプの画像、ビデオフレーム等にも等しく適用可能である。

【００３５】

（登録）

（画像捕捉）

一実装では、１つ以上の眼画像（および／または眼領域画像）は、７２０ｐ、１０８０ｐ、または同等／より高い分解能等、本明細書に説明される画像処理機能性のために好適な画質において、画像センサを用いて捕捉される。画像センサは、概して、携帯電話およびタブレットにおいて見出される、正面に面したカメラ等、例えば、１メガ画素またはより優れた画像センサであることができる。ユーザの眼は、例えば、ヴィオラジョーンズ法を使用して検出されることができ、ユーザの視線方向は、リアルタイムで全て検出されることができる。安定した視線および少なくとも片眼の検出に応じて、ユーザの眼の画像のスタックが、捕捉される。

【００３６】

入力スタックから空間的に位置合わせされた画像は、センサ雑音を低下させるために平均化され、最良の結果として生じる平均化されたショットは、無参照画質測定基準を使用して選択される。低または無光条件において、デバイス画面の背面照明と、前述の平均化に起因するマルチフレーム雑音低減とは、本明細書に説明されるバイオメトリック処理動作が実施されることを可能にする。一実施例では、容認可能量の相違（例えば、動きおよび瞬きに起因する）を超えないいくつかの連続画像フレーム（例えば、３つ、４つ、５つ、またはそれ以上）が、リアルタイムで位置合わせされ、平均化される。画像スタックは、ラプラシアンガウシアン（ＬｏＧ）ベースの品質測定基準（（鮮明化画像－オリジナル）の標準偏差）を使用してランク付けされることができ、上位ｎ個は、さらなる処理のた

めに留保される（例えば、確認のために最大２つ、登録のために最大４～６つ）。

【００３７】

（セグメント化および強調）

画像捕捉（および、行われる場合、平均化）に続いて、選択された画像は、緑色－青色スペクトルで血管をより良好に表すようにカラー処理され、以下、着目領域（ＲＯＩ）と称される眼の白色部分の輪郭を描くようにセグメント化されることができる。一実装では、画像は、複数の円錐断面曲線を眼瞼および角膜縁境界に合わせることによってセグメント化される。セグメント化有効性が、チェックされる（例えば、マスクは、ＲＯＩの境界ボックスの少なくとも４０％であるべきである）。一連の血管分布強調画像フィルタ処理、鮮明化、および適応コントラスト操作が、より特定のバイオメトリックテンプレートのために必要とされる改善された画像を提供する。例えば、画像の緑色（無赤色）層は、ＬｏＧにオリジナルを掛けたもののコントラスト制限付適応ヒストグラム均一化（ＣＬＡＨＥ）ならびに特別に調整された偶数ガボールフィルタバンクを使用して、強調されることができる。強調された画像の一連のマルチスケールかつ特別にフィルタ処理された適応物は、次いで、次のステップのために使用されることができる。

【００３８】

（着目点検出および特徴抽出）

各ＲＯＩに対して、着目点の場所（x_i、y_i）が、識別され、その数は、画質に応じて、典型的には、１００～４００に及ぶ。図３は、眼３００の血管系３１５の識別される着目点３２０を伴う、例示的眼内画像を描写する。着目点３２０は、２０１４年５月９日に出願された米国出願第１４／２７４，３８５号「Ｆｅａｔｕｒｅ Ｅｘｔｒａｃｔｉｏｎ ａｎｄ Ｍａｔｃｈｉｎｇ ｆｏｒ Ｂｉｏｍｅｔｒｉｃ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ」（その全体は、参照することによって本明細書に組み込まれる）に説明されるもの等の血管点検出器を使用して識別されることができる。着目点を検出する他の方法も、可能性である。

【００３９】

次に、血管の着目点場所（x_i、y_i）の周囲の局所画像パッチを統計的に（但し、正確または一意にではない）記述する、一組の

【数１０１】

$$\vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d$$

記述子ベクトルが、算出される。画像パッチ記述子の例は、限定ではないが、高速化ロバスト特徴（ＳＵＲＦ）、マルチ半径拡張型パターンローカルバイナリパターン（ＨＬＢＰ）（のヒストグラム）、およびマルチ半径拡張型パターン中心対称ローカルバイナリパターン（Ｈ　ＣＳ　ＬＢＰ）（のヒストグラム）を含む。各ＲＯＩに対して、検出された血管の着目点ＶＰＤを含む、未処理（非保護）バイオメトリックテンプレートT_{VPD}が、次いで、以下のように定義される。

【数１０２】

$$T_{VPD} = \{t_i\}, t_i = \left[(x_i, y_i), \vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d\right], i = 1,2, \ldots n(T_{VPD})$$

【００４０】

確認時、主張される識別に対して記憶された登録テンプレートが、提示される確認テンプレートに対してマッチングされる。一実装では、類似性スコアが、登録テンプレートと確認テンプレートとをまたがる、ある最小数の要素の対もまた必要とする事前に設定された閾値を上回る場合、主張者は、容認され、一致の決定が発行される。眼画像は、テンプレートの作成後、直ちに破棄され、登録テンプレートのみ記憶され得ることに留意されたい。

【００４１】

（難読化およびエンコード）

（チャフ点の追加およびタグ付け）

一実装では、バイオメトリックテンプレートをセキュア化の初期ステップは、T_{VPD}からの記憶されるべき登録テンプレート要素を、真正血管の着目点と同じまたは実質的に類似するように見える多数の人工的に合成された要素間に秘匿することを含む。これらの合成された要素は、本明細書では、「チャフ」と称される。一実装では、チャフの数は、実テンプレート要素ｎ（T_{VPD}）の数の約３～７倍である。しかしながら、他の倍数も、考えられる。例えば、より高いチャフ密度は、さらにより高いレベルの難読化を提供することができる（但し、さらなる算出負荷を犠牲にする）。

【００４２】

チャフ要素は、全データ点、すなわち、チャフおよび非チャフ（すなわち、実際の血管の着目点）の空間分布が、均一であるか、または血管の着目点と同一もしくは実質的に類似するパターンまたは分布に従うことを確実にするアルゴリズムによって挿入されることができる。一実施例では、（x_i、y_i）の局所空間密度は、所与の面積の微小区域またはタイルに至るまでほぼ同一であり、記述子のコンテンツまたは空間関係は、空間粒子内において実非チャフ（実際の血管の着目点）からチャフをあらわにしない。図４Ａは、約３倍のチャフ対非チャフ配置に関する、チャフ点（正方形）内に埋め込まれた図３からの血管の着目点（円形）を描写する。図４Ｂは、図３からのオリジナル眼画像上に重ねられた図４Ａからの難読化点の可視化である。しかしながら、眼画像は、この難読化段階に先立って、かつT_{VPD}の計算直後に破棄され得ることに留意されたい。

【００４３】

各テンプレート点t_iは、実（血管の着目点）か合成（チャフ）かにかかわらず、２つのタイプの情報、すなわち、場所（ｘ、ｙ）およびパッチ統計Ｖを含むことができる。チャフデータ点の判別不能性のためのチャフ注入テンプレートの空間均一性は、いくつかの手段によって達成されることができる。一実装では、以下の２ステップチャフ（ｘ、ｙ）場所生成プロセスが、使用される。ステップ１（粗チャフ配置）では：登録テンプレートの空間スパンにわたる典型的タイリング（例えば、４×５）が与えられると、タイルあたりの合計テンプレート点（チャフおよび非チャフ）の平均を均等にするために必要なチャフの第１の部分を配置することから開始し、目標数は、任意のタイルにおいて、ＶＰＤ点の最大数を上回る。タイルあたりの血管の着目点ＶＰＤ＋チャフ点密度目標の約５０％に到達するまで継続する。この粗チャフ化ステップのために、全データ点（チャフまたは血管の着目点）間に初期最小距離要件（例えば、３画素）を使用する。ステップ２（細チャフ配置）では：チャフの残りの挿入を継続し、タイルあたりの所望の均一血管の着目点ＶＰＤ＋チャフ点密度目標の１００％を達成するまで、最小距離閾値を低減させる（例えば、１画素まで）。

【００４４】

一実装では、１．２ＭＰカメラによって作成されるデータ点場所に対する（ｘ、ｙ）範囲の低端は、約８０×１００画素＋／－２０である。しかしながら、この数は、カメラの視野、被写体距離、および他の要因に基づいて、変化し得ることに留意されたい。本方法および他の代替方法の詳細は、以下の「サンプルチャフ生成およびタグ付け関数実装」と題されたセクションに説明される。

【００４５】

チャフ配置に続いて、チャフ記述子ベクトル

【数１０３】

$$\vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d$$

が、真正血管の着目点ＶＰＤに関連付けられた記述子と同様に合成される。すなわち、チャフ点に割り当てられる記述子のコンテンツは、実着目点ＶＰＤのために導出されるものと統計的に類似し、それと判別不能であるように形成される。チャフ記述子と実血管記述子の前述の判別不能性は、種々の様式において達成されることができる。一実装では、登録中に種々のチャフ記述子を生成するために、小ランダム循環シフトおよび追加の雑音が、その実対応物のものと同一の統計的分布に従うチャフ記述子を得るように、実血管記述

子に適用される。これらの特徴は、以下に説明されるように、後に、「スクランブリング」されることができる。

【００４６】

登録テンプレート作成時、チャフ点およびその合成記述子は、テンプレートの実ＶＰＤスパン部分のように構造化される。

【数１０４】

$$T_{CHF} = \{t_i\}, t_i = \left[(x_i, y_i), \vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d\right], i = 1,2, \ldots n(T_{CHF})$$

チャフ注入難読化テンプレートは、したがって、以下によって与えられる（順不同）集合の形態となる。

【数１０５】

$$T_A = T_{VPD} \cup T_{CHF}$$

【００４７】

「タグ付け」機能は、１つのテンプレート要素の別のものへの一方向マッピングである。具体的には、タグ付け関数は、チャフ難読化テンプレート内のテンプレート点に、そのテンプレートからの所与の任意の他のデータ点を見出す、または「タグ」付けするために使用されることができる。一実装では、タグ付け関数f_Tは、以下の特性を満たす：（１）そのドメインは、

【数１０６】

$$\left\{\left[(x_i, y_i), \vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d\right]\right\}$$

を含む：（２）非自明かつ多対一である（または、別様に不可逆的または既知もしくは事実上の逆数を伴わない）（例えば、スクランブリングおよびエンコード／デコード状態において、ならびにタグ付けのために使用され得る、ＳＨＡ５１２ハッシュ関数に基づいて）：および（３）所与の登録テンプレートにわたって、範囲が、血管の着目点の集合と最小限に交差すること（すなわち、テンプレートの血管の着目点の部分集合内に最小限の自己タグ付けが存在する）：

【数１０７】

$$\frac{n(f_T(VPD) \cap VPD)}{n(VPD)} \ll 1$$

【００４８】

そのような関数の本実装および代替実装は、「サンプルチャフ生成およびタグ付け関数実装」と題されたセクションに説明される。テンプレートのＶＰＤ部分に対する公称値が与えられると、これらのタグ付け関数は、概して、それらの入力時における各血管の着目点あたり、それらの出力時における約１つの点をタグ付けする。一実装では、タグ付け関数は、チャフのキーエンコード部分集合（以下参照）とチャフの信頼サーバシグネチャ担持部分集合（以下の「信頼サーバ機能性」参照）とをタグ付けするために使用されることができる。これらの２つのタグ付け関数は、その範囲においてわずかな重複を含み得る。

【００４９】

本明細書に説明されるようなタグ付け関数f_Kは、テンプレートの実T_{VPD}部分がマップするテンプレート点T_K（タグ付け関数の第３の特性を前提とすると、大部分はチャフ）を見出すために使用されることができ、$T_K = f_K(T_{VPB})$である。図５は、タグ付けされた点の部分集合（塗り潰された円形および正方形）とともに、図４Ａからの実点（円形）および難読化点（正方形）を描写する。随意に、テンプレートの別の類似する（但し、同じではない）部分集合が、設計またはメタパラメータにおける差異だけf_Kと異なる、第２のタグ付け関数f_Sを使用してタグ付けされ、随意の信頼サーバ機能性のために使用され得る、$T_S = f_S(T_{VPD})$をもたらすことができる。

【００５０】

T_Kは、次いで、秘密キーをエンコードするために使用されることができる。T_{VPD}は、登録プロセスの間、かつT_{CHF}におけるその難読化の前のみ既知であることに留意されたい。T_{VPD}の記録は、保持されず、T_{VPD}の部分集合のみ、真正バイオメトリック確認成功の際にあらわにされる。

【００５１】

（記述子のスクラングリング）

一実装では、次元性を低減させ、マッチングの正確度およびスピードを改善し、脱相関し、したがって、チャフ難読化登録テンプレートの均一性をさらに「平坦化」および強化するために、異なる特徴ベクトル

【数１０８】

$$\{\vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d\}, i = 1,2, \ldots, n(T_A)$$

の主成分分析（ＰＣＡ）投影のための負荷が、大量の代表的訓練集合を使用して事前に計算され、記憶される。次に、チャフ注入テンプレート内の記述子は、スクリーグラフ分析を使用して、それらのオリジナルの説明される変化の有意性（例えば、８０％を上回る）を保ちながら、そのオリジナル長さのある割合、例えば、約３０％まで低減される。平均減算法後のＰＣＡ投影の随意の分散正規化は、全てのその特徴にわたって対角正規化共分散行列を有する、白色化され記憶されるテンプレートを作成する。ＰＣＡの特性を与えられると、結果は、マッチングのために必要なほとんどのユークリッド距離情報を保存する。最後に、スクランブリングプロセスが、異なるソフトウェアおよびデバイスハードウェアシグネチャのハッシュを使用して、（ａ）全記述子に追加されるＳＨＡ５１２導出バイアスベクトルを使用して、ＰＣＡ短縮特徴を改変するためのソルト付与プロセス（登録および確認テンプレートの両方に対して、登録テンプレートのための保存に先立って）と、（ｂ）結果として生じる特徴ベクトルの座標のシード変調並べ替え（登録テンプレートのための保存に先立って）とをシードすることができる。

【００５２】

ロッシーＰＣＡ投影に加え、（ａ）および（ｂ）は両方とも、ユークリッド距離を保存し、ユーザのデバイスに結び付けられたスクランブリングされた空間内でマッチングを行うことを可能にすることに留意されたい。これは、等長（距離保存）かつ取り消し可能なサロゲート空間内のマッチングが、セキュアかつプライベートなバイオメトリックパターンマッチングに重要であるため、特に着目に値する属性であり、かつデバイスおよび真正ユーザの両方が、前述のバイオメトリック認証を成功させるために必要とされるであろうため、２要因認証につながる。マッチング中、記述子のスクランブリング解除が不要である（したがって、露出のリスクを回避する）だけではなく、独特のソフトウェア取り消し可能かつデバイス特定のスクランブリング空間が、バイオメトリック認証アプリケーションの各インストールに対して及ぼされることができる。

【００５３】

（キーエンコード）

キー生成（すなわち、バイオメトリックマッチの副産物として秘密キーを算出すること）のための拡張テンプレート構造の一実装が、ここで説明される。次数ｋの線形方程式系があり、その係数は、秘密の数値

【数１０９】

$$\vec{S}, (\dim(\vec{S}) = k$$

と見なされると仮定する。確認中、ｋは、経験的０％誤受入率（ＦＡＲ）閾値（すなわち、利用可能な最大バイオメトリック眼読み取りデータ集合を使用した、いかなる偽物も受け入れない決定閾値）で動作する、真正ユーザの登録テンプレートと確認テンプレートとの間のマッチングプロセスの成功中に見出される最小数の血管の着目点である。線形方程式系は、順序付けされた組のデータ点が、そのキーを解くために要求されないため、キーをエンコードするために使用されることができる（キーは、その複雑、難解、かつ高エン

トロピの構造から生じる、眼静脈パターンマッチングの高感度および特有性を前提として正確に解かれる、線形方程式系に直接エンコードされることができる）。

【００５４】

したがって、一組のデータ点

【数１１０】

$$D = \{d_i\}, n(D) \geq k$$

が、キーを構成するｋ個の未知数を解くために必要とされるｋ個の方程式の復元につながる真正確認成功によって可能にされる、線形方程式系を一意に解き、エンコードされた秘密の数値ベクトル

【数１１１】

$$\vec{S}$$

を読み出すために必要される（キービット列フローの観点から、標準的長さおよび強度をさらに強化するために、ＳＨＡ５１２が、パターン予測不能５１２ビットプライベートキー列を有するように、このキーの演算子バージョンに適用され得る）。復元されるマッチング点の順序、したがって、方程式の順序は、問題ではないことに留意されたい。キー生成情報は、チャフ難読化登録テンプレートの拡張（関数適合のための記述子投影値を伴う）要素の部分集合にわたって内部分散される。チャフ難読化登録テンプレートは、以下T_{AK}と称され、以下のように定義される。

【数１１２】

$$T_{AK} = \{t_i\}, t_i = \left[(x_i, y_i), \vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d, \vec{Y}_i^1, \vec{Y}_i^2, \ldots \vec{Y}_i^d\right], i = 1,2, \ldots n(T_A)$$

式中、（x_i、y_i）は、T_A内の着目およびチャフ点ｉの場所である。テンプレートの拡張部分は、

【数１１３】

$$\vec{Y}_i^1, \vec{Y}_i^2, \ldots \vec{Y}_i^d$$

であり、ベクトルの集団は、次元性において

【数１１４】

$$\vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d$$

に類似するが、Ｙの各要素は、ｋ方向ベクトル化関数（以下の「ベクトル化関数」参照）を使用したＶからの対応する要素の投影であり、次いで、

【数１１５】

$$\vec{S}$$

との内積演算は、前述の方程式系の右側を提供する。（

【数１１６】

$$\vec{V}$$

の各要素は、異なる

【数１１７】

$$\vec{S}$$

をエンコードすることに留意されたい）。秘密ベクトル

【数１１８】

$$\vec{S}$$

（の集合）は、後に、真正ユーザによって、バイオメトリック認証成功に応じて読み出さ

れる。前述のプロセスは、以下のエンコードおよびデコードステップを通して説明され、それらのステップは、数値安定性を維持しながら、セキュリティおよびプライバシーを向上させるためのタグ付けおよびベクトル化関数によって可能にされる。

【００５５】

（エンコードプロセス）

一実装では、キー生成機能性は、判別不能チャフによって難読化されたときでも、登録テンプレートと確認テンプレートとの間に少なくともｋ個の一致した点をもたらす真正受入成功（真の正確認）に基づく。したがって、ｋ個の未知数を伴うｋ個の方程式系は、このマッチングプロセスの上に成り立ち、方程式のためのｋ個のデータ点は、事実上、真正マッチング成功を通してのみ既知となり得、方程式、したがって、キーは、真の一致が生じた場合のみ、一意に解かれることができる。

【００５６】

ｋは、画質およびマッチャ強度の関数であり、いずれかに対する改善に伴って増加されることができること、または、複数のＲＯＩ／テンプレート（登録および確認バンクからの）と複数の登録テンプレート内の同一のエンコードされたキーをマッチングし、方程式を解法し、秘密キーを復元する前に、見出されたタグ付け点の和集合をとることによって、増加されることができることに留意されたい。

【００５７】

一実施例では、経験的ＦＡＲ＝０閾値において収集されたデータ集合にわたる観測を前提として、単一視、単一比較、２－ＲＯＩマッチングに対して、ｋ＝４０である。一致した点は、テンプレートエントリであり、テンプレートエントリは、それらの記述子の近接性を通して、それらの対応する確認対応物と比較された後、かつランダムサンプルコンセンサス（ＲＡＮＳＡＣ）をアフィン変換仮説（または、類似物）とともに使用して、外れ値の拒否後に選択される。そのような一致したテンプレートエントリの数が、ｋまたはそれより大きい場合、誤受入は、生じない（すなわち、生成または公開される秘密は、観測の境界内のその閾値において、各ロック解除ユーザに対して独特である）。感受性が低いアプリケーションに対して、マッチャが破損または侵害されていないと仮定される場合、マッチャが要求を拒否していることを前提として、キー生成段階における誤受入イベントは進行しないであろうと仮定し（すなわち、マッチスコアが一致した点の数より高い感度および特有性を有すると仮定して、一致した点の数が、ｋをわずかに下回るが、マッチスコアが一致を示す場合）、より小さいｋが、キー生成誤拒否率を低減させるために使用されることができる。

【００５８】

キー生成を継続すると、チャフ難読化テンプレート作成時、

【数１１９】

$$T_A = T_{VPD} \cup T_{CHF}$$

が、もたらされる（T_{VPD}、T_S、およびT_K間にわずかな重複が存在し得る）。f_K（T_{VPB}）によってタグ付けされたチャフのT_K部分集合が、T_Kのコンテンツおよび線形方程式系を使用して、１つ以上の（ランダム）秘密キー

【数１２０】

$$\vec{S}$$

をエンコードする関数（例えば、線形投影）に提供される。ＶＰＤ部分集合

【数１２０－１】

$$i = 1,2,\ldots,n(VPD)$$

からの各タグ付け血管要素あたり（約）１つのタグ付けされた点

【数１２１】
$$t_i \in T_K$$

が存在すると仮定する。キーエンコードプロセスは、全ての異なる記述子集合（例えば、ＳＵＲＦ、ＬＢＰのヒストグラム等）に対して類似し得るため、プロセスは、１つの一般的タイプのそのような特徴に対して実証されることができる。

【００５９】

簡略化されてはいるが、拡張された形態の

【数１２２】
$$T_A = T_{VPD} \cup T_{CHF}$$

（単一タイプの記述子を使用し、チャフ注入される）を仮定すると、Ｔは、以下となる。

【数１２３】
$$T = \{t_i\}, t_i = \left[(x_i, y_i), \vec{V}_i\right]$$

V_iの次元性がＤである場合、以下のように、秘密キーの行列$W_{D \times k}$＝［$W_{j\,d}$］としてＤ×ｋ個の数値（実数またはその他であり、各行は、異なるキーベクトル

【数１２４】
$$\vec{S}$$

と見なされ得る）から成る任意のキー行列Ｗをエンコードすることができる。

【数１２４－１】
$$T_A, v_{i,d}, d = 1,2, \ldots D, i = 1,2, \ldots n(T)$$

内の特徴ベクトルV_iのＶＰＤ部分集合の各スカラー要素は、非自明かつ不可逆的ベクトル化関数を使用して、ｋ個の特定の値にベクトル化（分割）される。ベクトル化（スプリッタ）関数は、したがって、以下を行う。

【数１２５】
$$\vec{X} = \vec{\varphi}(x), \quad \dim(x) = 1, \dim\left(\vec{X}\right) = k$$

【００６０】

ベクトル化関数を伴わない簡易バージョンも、可能であり、その場合、Ｄ≧ｋ（したがって、Ｄではなく、各拡張された

【数１２６】
$$\vec{V}_i$$

あたり１つのY_i）であるとすると、最大次元性Ｄのキーベクトルは、各

【数１２７】
$$\vec{V}_i$$

の線形組み合わせとして直接エンコードされる。しかしながら、デコードプロセスのためのｋ個の並置された

【数１２８】
$$\vec{V}_i$$

の行列は、特異であるべきではない。

【００６１】

最後に、対応する$y_{i,\,d}$が、

【数１２９】

$$y_{d,i} = f_{encode}(\vec{W}_d, v_{d,i}) = \vec{W}_d \cdot \varphi(v_{d,i})$$

によって

【数１３０】

$$\vec{W}_d$$

（ｋの長さを伴う秘密キー行列Ｗの行ｄ）をエンコードする入力ｖ$_{i,d}$に関連付けられ、追加される。

【００６２】

前述の列は、

【数１３１】

$$\vec{Y}_i\text{-}$$

拡張

【数１３２】

$$T_K\text{:}\{[(x_i, y_i), \vec{V}_i, \vec{Y}_i]\}$$

を求めるために、記述子／キー集合

【数１３３】

$$\vec{V}_i, \vec{W}_d$$

の全Ｄ次元、およびキー生成のためのテンプレートの全ｎ（Ｔ$_K$）ｆ$_k$－タグ付け要素に対して繰り返される。次に、Ｗが、Ｗ$_c$に達するように改変され（わずかな雑音を追加することによって最小限に）、同様の適用が、ｙ$_{i,d}$を含むその構成要素が、タグ付け、非タグ付け、チャフ、および血管要素にわたって一緒に完全に混合するような完全｛ｙ$_{i,d}$｝－拡張Ｔを求めるために、テンプレートのｆ$_k$－非タグ付け部分に行われる。複数の偽Ｗが、もたらされ、各々は、Ｔ$_{AK}$の部分集合（さらなるセキュリティのために推奨されるｎ（Ｔ$_{VPD}$）数の要素を伴う部分集合）に適用される。

【００６３】

前述のプロセスは、不可逆的、すなわち、ｙ$_{i,d}$を所与とすると、ｖ$_{i,d}$および

【数１３４】

$$\vec{W}_d$$

に戻ることができないことに留意されたい（一例を挙げると、

【数１３５】

$$\vec{\varphi}(x)$$

およびｙ$_{d,i}$の計算は、多対一関数かつ不可逆的であって、さらに、正の真正確認時まで、Ｔ$_{AK}$のどの部分集合が、タグ付けされたデータ、したがって、それを解くためにＷ－エンコードされたデータを含むかが分からない）。

【００６４】

一観測実施例では、ｋ＝４０（単一視、単一比較、２ＲＯＩ）の閾値を伴うデータ集合内には、誤受入は、もたらされることはなかった。すなわち、観測限界内では、２人の異なるユーザは、同一キーを生成せず、したがって、エントロピは、表面上、キー長に等しいと思われる。しかしながら、これは、はるかに大量のユーザデータベースに対して、ｋ＝４０における衝突（誤受入）が生じる可能性がないことを含意するものではなく、その場合、単に、ｋを増加させてもよい（但し、より高い閾値を与えると、おそらくより高い誤拒否率を犠牲にする）。経験的誤受入率評価に関して、地球上の全７０億人の人口を使用して、最大わずか約３６ビットに対するバイオメトリックキー空間の一意性を実験的に

保証することができる（ｌｏｇ$_2$（７×１０ｅ９）＝３６．０３）。前述を前提として、ｋに対するある任意の厳密な閾値では、Ｔ$_{ＡＫ}$のチャフ誘発難読化のレベルは、最終的に、キーエントロピに対する限界を構成するであろう。

【００６５】

エンコードされたキーは、Ｗまたは対応する｛Ｙ$_i$｝のコンテンツの変更から、ベクトル化関数の変更まで、複数の異なる方法において、変更、置換、または取り消されることができる。タグ付け関数およびチャフコンテンツもまた、前述を達成するために変更されることができる。これらの方法のうちのいくつかは、登録時に適用可能である一方、その他は、随時、適用されることができる。例えば、随時、各ベクトルキー

【数１３６】

$\vec{W}_d$

は、ｉにわたりｙ$_{ｄ，ｉ}$の少なくともｎ（Ｔ$_A$）－ｋ＋１個の要素に摂動を与えることによって、例えば、小雑音ベクトルを｛Ｙ$_i$｝の全てのｄ番目の要素に追加することによって、プライベート、セキュア、かつ便宜的方法において、取り消しまたは変更されることができる。これは、その新しいまたは古いコンテンツをあらわにせずに、解

【数１３７】

$\vec{W}_d$

を変更し、解は、真正ユーザの確認成功によって可能になるＴ$_k$の少なくともｋ個の要素の発見に応じてのみ既知となり得る。複数の登録テンプレートおよびＲＯＩの場合、同一キーＷが、各テンプレートにおいてエンコードされることができ、その結果、最良／組み合わせ比較から公開されるキーは、同一のままである。タグ付けされたテンプレート要素は、これらの登録にわたって異なるので、対応する｛Ｖ$_i$、Ｙ$_i$｝もまた、異なり、したがって、同一のエンコードされたＷを有する複数のテンプレートの比較から生じる攻撃ベクトルは、存在しないことに留意されたい。

【００６６】

（確認およびデコード）

一実装では、バイオメトリックテンプレート確認は、登録プロセスに関して前述のものと同一または実質的に同一様式における、画像捕捉、セグメント化および強調、着目点検出および特徴抽出、ならびに記述子スクランブリングから開始する。一方、チャフの追加およびタグ付けならびにキーエンコードは、登録プロセスにのみ適用される。

【００６７】

（マッチング）

マッチング中、記憶された登録テンプレートによって表されるような主張される識別は、登録テンプレートを同一スクランブリング空間内の確認テンプレートに対してマッチングすることによって、確認されることができる。成功する場合、登録テンプレートからの少なくともｋ個の血管の着目点が、正の真正一致の結果として、正しく見出される。これは、キーエンコードの逆であるが、それに類似する、キーデコードプロセスを可能にする。デコードは、Ｗを算出するためのｋまたはそれより大きい濃度（ｃａｒｄｉｎａｌｉｔｙ）を伴うＴ$_{ＡＫ}$の部分集合の発見を可能にする。

【００６８】

テンプレート間攻撃を抑制するために、機略に優れた攻撃者が、デバイス、そのコード、および論理を侵害し、複数の登録テンプレートへのアクセスを得て、それらをクロスマッチングしようとする場合、攻撃は、互のマッチング距離内に異なるテンプレートにわたりチャフコンテンツ（または、登録テンプレートに追加されるべきそれぞれのチャフ記述子を合成するときの、以前のテンプレートの任意の有意な部分）を有することによって、阻止されることができる。

【００６９】

テンプレートマッチングアルゴリズムの一実装は、以下のように簡単に説明される。（

１）画像ピラミッドが、マルチスケールマッチングプロセスのために形成される。（２）着目点が、血管点検出器を使用して見出される。（３）特徴が、前述の点の周囲のマルチ半径ＬＢＰ（ローカルバイナリパターン）、マルチ半径ＣＳ－ＬＢＰ（中心対称ＬＢＰ）、ＳＵＲＦ、Ｈ－ＬＢＰ（ＬＢＰのヒストグラム）、およびＨ－ＣＳ－ＬＢＰ（ＣＳ－ＬＢＰのヒストグラム）を使用して、計算される。結果は、未処理登録テンプレート（前述のように、一組の（ｘ、ｙ）血管点座標に加え、それらの周囲の画像パッチのための記述子ベクトル）として保存される。（４）記述子が、事前に計算されたＰＣＡ負荷を使用して、短縮および脱相関され、等長でスクランブリングされる（デバイス特定のソルト付与および次元のリシャッフリング）。マッチングが、このサロゲートプライベート空間内で行われる。（５）登録および確認テンプレート点間の最近傍マッチが、加重和を使用して、登録－確認点対の周囲の全記述子のユークリッド距離に基づいて、見出される。候補対は、以下の外れ値拒否ステップに渡される。（６）アフィン／無反射相似仮説を伴うＲＡＮＳＡＣは、仮定される幾何学的変換仮定ならびに関連変換行列に従って、外れ値を見つけるために行われる。（７）最終マッチスコアが、外れ値が除外された登録－確認一致対のｘおよびｙ座標、見出された対の数（ｋ）、およびＲＡＮＳＡＣから復元されたスケールおよび回転（または、合理的値以外の識別からの変換行列の偏差を合計する他の測定基準）の相関の非線形関数として見出される。

【００７０】

（キーデコード）

一実装では、確認テンプレートは、最初に、真正マッチ成功に応じて、T_{VPD}のｋ個以上の元を見つけるために、拡張および難読化された登録テンプレートに対してマッチングされる。各バイオメトリックトランザクションに対して複数のＲＯＩまたは登録／確認テンプレートを使用する場合、ｋ個以上の一致した点にヒットした第１の比較が、エンコードされたＷを算出するために使用されることができる。より多くのｋを達成するために、そのような複数の比較を通して見出される、タグ付けされ、拡張された登録要素の和集合をとることもできる。

【００７１】

次に、タグ付け関数f_kを使用して、T_Kからの点のうちのｋ個以上の点が、識別される。これらの点は、設計上、Ｗ－エンコード関数f_{encode}上にある。ｋ個の点のみ、結果として生じる方程式系の厳密解のために必要とされ、したがって、確認成功プロセスからの第１のｋ個（または、復元されたT_Kの任意の他のｋ個の元）が、使用されることができる。T_Kの前述のｋ個の元の各々に対して、それぞれの$v_{i,d}$が、以下の「ベクトル化関数」に説明されるものと同一ベクトル化（スプリッタ）関数を使用して、ｋ個の構成要素にベクトル化される。それらの対応する$Y_d=[y_{i,d}]$に沿って、ｋ－方向にベクトル化された$v_{i,d}$（ｉ＝１，２，・・・ｋ）は、以下のように、それらの対応するエンコードされたキー

【数１３８】

$$\vec{W}_d(w_{i,d}, i=1,2,\ldots k)$$

を見出すための十分な情報を有する。すなわち、各行ｄに対して、$v_{i,d}$のｋ個のサンプル（ｉ＝１，２，・・・ｋにわたって反復される）が、前述のベクトル化関数φによって、ｋ方向に分割され、$[\varphi]_{k\times k}$を生じさせる。キーベクトル

【数１３９】

$$\vec{W}_d$$

が、次いで、以下のエンコードファクトを使用して見出される。

【数１４０】

$$[\varphi]_{k\times k}[w_d]_{k\times 1}=Y_d$$

したがって、以下となる。

【数１４１】

$$[w_d]_{k\times 1} = [\varphi]^{-1}_{k\times k}\, Y_d$$

再び、ｋ個のデータ点が、方程式解法のために使用されるため、順序は、問題ではなく、ｋの濃度を伴うＴ$_{K}$の任意の部分集合で十分となるであろうことに留意されたい。前述の簡易バージョンを使用するデコードは、同様の論理に従うが、ベクトル化関数を伴わない。

【００７２】

初期セキュリティ分析が、ここで説明される。以下は、テンプレートが解読され、バイオメトリック認証コードが逆コンパイルされた、侵害されたデバイスを仮定する。秘密キー担持チャフＴ$_{K}$（約ｎ（Ｔ$_{VPD}$）個の元を伴う）が、テンプレート要素の残りと判別不能であるとすると、Ｔ$_{K}$の元を表す当たりくじを引く可能性は、約ｎ（Ｔ$_{K}$）／ｎ（Ｔ$_{A}$）である。全ての要求されるｋ個の点を推測するための総当たり攻撃は、盗まれ、暗号化されていない登録テンプレートおよびプログラム論理を仮定して方程式系を解くためのそのような推測の独立し、同じく分布された性質に加え、成功手段の可用性を考慮すると、ほぼ、

【数１４２】

$$\left(\frac{n(T_K)}{n(T_A)}\right)^k$$

である。何故なら：

【数１４３】

$$P(guess_1 \in T_K, guess_2 \in T_K, \ldots guess_k \in T_K) = \prod_{i=1}^{k} \frac{n(T_K)-i}{n(T_A)-i} < \left(\frac{n(T_K)}{n(T_A)}\right)^k$$

【００７３】

したがって、有効エントロピは、以下のように計算され得る。

【数１４４】

$$\text{エントロピ} = -k\log_2\left(\frac{n(T_K)}{n(T_A)}\right)$$

例として、ｋ＝４０の最小真正一致点と、１／５（血管の着目点あたり約４つのチャフ点）の合計テンプレート点に対する典型的数のチャフの比率とを用いると、エントロピは、９２ビットより大きい。

【００７４】

系の容量、すなわち、キーＷのサイズは、Ｄ×ｋ×Ｌビットであって、式中、Ｌは、Ｗをエンコードするために使用される数系の長さ（ビット単位）であることに留意されたい。例えば、ＳＵＲＦ－１２８特徴（ＳＵＲＦの１２８次元バージョン）のみを使用し、かつＷを表すための符号なしの６４ビット整数フォーマット（切り捨て誤差を抑制するためにＬＳＢを破棄した後、６３有効ビット）を使用すると、キー容量（長さ）は、１２８×３６×６３＝２９０，３０４ビット、すなわち、約３５ＫＢである。しかしながら、これは、前述で計算されるような系のエントロピではない。キービット列フローの観点から、標準的長さおよび強度を強化するために、ＳＨＡ５１２は、各エンコードされるキーＷ$_{D}$に適用されることができる。したがって、Ｗ$_{D}$のサイズにかかわらず、パターン予測不能な５１２ビットプライベートキー列が存在する。

【００７５】

（サンプルチャフ生成およびタグ付け関数実装）

タグ付けおよびチャフの使用は、続く機能性を、血管系によって及ぼされた（すでにスクランブリングおよび難読化された）実テンプレート点および記述子から切り離し、さら

なるセキュリティ、プライバシー、および取り消し可能性を提供する。以下は、チャフ、その生成、およびタグ付けの種々の実装に関するより具体的詳細を提供する。

【００７６】

（チャフの空間配置）

空間的に均一または別様に血管着目点と判別不能な「チャフ注入」は、記憶されたテンプレートを保護するためのいくつかの方法で達成されることができる（概して、確認テンプレートとしての登録テンプレートは、マッチング中に瞬間的に生成される）。一実施例では、実（非チャフ）着目点間の最小（外れ値が拒否される）空間距離が、決定される。チャフ点は、任意の２つの点（チャフおよび／または血管の着目点）間の距離がほぼ同一最小距離となるまで挿入される。高密度にチャフ注入されたテンプレートは、複数の前線（ｆｒｏｎｔ）により強固なセキュリティをもたらすであろう。不都合な点は、チャフ難読化テンプレートのより大きいサイズであり、これは、マッチャを減速させ得る。

【００７７】

別のあまり極端ではない実装は、２ステップチャフ挿入である。より具体的には、登録テンプレートの空間スパンにわたる典型的タイリングを所与として、粗チャフ挿入として知られる、このステップのための最小距離要件（例えば、３画素）を使用して、チャフの第１の部分の配置から開始する（面積微粒子、すなわち、チャフおよび非チャフあたりの合計テンプレート点の平均をほぼ等しくするために必要とされる）。プロセスは、最小距離閾値を緩和する（例えば、１画素まで）ことによって、所望のチャフと非チャフの比率、典型的には、３ｘ対７ｘを達成するまで、チャフの残りの挿入を継続する（細チャフ挿入ステップ）。

【００７８】

チャフ配置のためのさらなる方法は、既存のテンプレートを使用し、チャフを空の場所／近傍に挿入しながら、非（または、ほぼ非）血管タイルの上に血管タイルにおける血管点の空間パターンを複製し（ある場合には、わずかな自然に生じた幾何学的歪曲を伴う）、タイル境界におけるチャフが投入されたテンプレートのｘ、ｙ座標の空間分布の連続性ならびにタイルあたりの全体的均一空間密度を観察することを含む。

【００７９】

さらに別の方法は、最近傍ドットが近すぎる場合、Ｌ－システム（ツリー状構造のためのリンデンマイヤー文法）を使用して、同一血管ツリー状構造に従うことを含む。次いで、チャフが、タイル境界における連続性を観察しながら、テンプレートにわたる均一タイル密度に達するまで、Ｌ－システム生成空間パターンに従って、あまり血管がないタイルに追加される。

【００８０】

（チャフ記述子コンテンツ）

一実装では、テンプレート内の記述子特徴ベクトルは、信号として見なされる場合、非エルゴード的プロセスである。チャフ注入された登録テンプレート内の各特徴要素の統計的特性はまた、空間および特徴空間内において、どれがその前後に来るかに関しても、チャフ対非チャフ記述子に対して同一であるべきである。記述子間距離の分布ならびにチャフおよび非チャフ内とそれらにわたるその平均および共分散行列もまた、類似すべきである。前述は、記述子（チャフおよび非チャフ）をゼロ平均および非相関にする、ＰＣＡ投影によって達成されることができる。前述の境界内では、血管点により近い場所のチャフ記述子は、互に対して一致する可能性が低く、したがって、マッチング正確度が損なわれない（ＶＰＤ記述子分布特性内に残りながら）ように選定されることができる。チャフ記述子コンテンツを既存の実点記述子から作成すること（例えば、ＶＰＤに関連付けられた特徴ベクトルへのわずかな循環シフトとわずかな雑音の適用）に加え、ＰＣＡ投影およびスクランブリング関数はさらに、チャフと真正記述子との間の任意の差異を平坦化するであろう。スクランブリングは、デバイス特定の様式において、ソルトを付与し、座標を並べ替え、所与の独特のソフトウェアおよびハードウェア環境内においてのみ、スクランブリングされた空間内に、マッチング目的のために、ユークリッド距離を保存し、単一バイ

オメトリック眼スキャントランザクション中の２要因認証を可能にすることに留意されたい。ＰＣＡステップの固有ベクトル投影後の随意の固有値正規化は、さらなるセキュリティのために、全てのその特徴にわたって、識別に近い共分散行列を有する、白色化され、記憶されるテンプレートを作成する。

【００８１】

（タグ付け）

タグ付け関数は、ハッシュ関数等を使用することによって、多くの異なる方法で実装されることができる。例えば、着目点のｘ、ｙ座標およびその対応する特徴ベクトルを仮定すると、（１）ｘ、ｙ座標は、それぞれの着目点に対応する局所特徴ベクトルＶの最初の８つの要素で追加される。（２）結果はＳＨＡ５１２を用いてハッシュ化される。結果として生じるビットストリングは、６４バイトにグループ化される。（３）タグ付けされた（出力）座標を導出するために、２組の列が、全奇数バイト場所を１つの列（Ｓｅｑｌ、３２バイト）および全偶数場所を第２の列（Ｓｅｑ２、３２バイト）として見なすことによって、前述のバイトストリングから抽出される。（４）Ｓｅｑｌ内の全バイトは、タグ付けされたｘ座標のための単一バイトを得るために、ビットＸＯＲ演算される。同様に、Ｓｅｑ２内の全バイトは、タグ付けされたｙ座標として単一バイトを得るために、ＸＯＲ演算される。（５）前述の場所にチャフ点が存在する場合、「タグ付け」されるであろう。そうでなく、最近傍チャフが、ｒ個の画素（例えば、１画素）の半径にある場合、選択は、計算された場所に移動し、タグ付けされる。前述のいずれも生じない場合、タグ付けされたチャフ点が、本場所において作成される。ＳｅｑｌおよびＳｅｑ２の異なる再ハッシュ化は、ｘ、ｙ範囲が、０－２５５を越える場合に実装されることができる。

【００８２】

別のアプローチは、タグ付け場所のための数学関数を使用することである。カスケード式に適用される３ステッププロセス（以下のＴｌ、Ｔ２、およびＴ３）を仮定する。入力テンプレート点の（ｘ、ｙ）座標は、以下のように変換される。

Ｔｌ：

【数１４５】

$$x_{new} = x\sin(y)$$

$$y_{new} = x\cos(x)$$

Ｔ２：

【数１４６】

$$x_{new} = \begin{cases} x < 1 & \text{の場合} \quad -x \\ x > x_{max} & \text{の場合} \quad x - x_{max} \\ x = 0 & \text{の場合} \quad 1 \\ \text{他} & \quad x \end{cases}$$

$$y_{new} = \begin{cases} y < 1 & \text{の場合} \quad -y \\ y > y_{max} & \text{の場合} \quad y - y_{max} \\ y = 0 & \text{の場合} \quad 1 \\ \text{他} & \quad y \end{cases}$$

x_{max}およびy_{max}は、チャフが投入されたテンプレート内の空間座標に対する最大値である。

Ｔ３：

【数１４７】

$$x_{new} = \begin{cases} x\text{が奇数の場合} & x_{max} - x \\ \text{他} & x \end{cases}$$

$$y_{new} = \begin{cases} y\text{が奇数の場合} & y_{max} - y \\ \text{他} & y \end{cases}$$

【００８３】

タグ付け関数は、バイオメトリック認証アプリケーションの異なるインスタンス化にわたって、挙動を変更するためにカスケード化または再パラメータ化されることができることに留意されたい。チャフ配置は、ＲＯＩマスク（より具体的には、個人の眼瞼輪郭を秘匿するために、全ＲＯＩマスクの和集合）に限定されることができる。

【００８４】

（チャフ場所およびコンテンツ合成のための例示的アルゴリズム）

チャフ場所およびコンテンツ合成のためのアルゴリズムの一実装は、以下の通りである。それらのそれぞれの記述子（一般に、ＨＬＢＰ、Ｈ　ＣＳ　ＬＢＰ、およびＳＵＲＦ）に沿ったＮ個のオリジナル（ＶＰＤ）点が存在し、サイズＲ×Ｃ画素（式中、Ｒは、行の数であり、Ｃは、列の数である）の画像からテンプレートを作成することを検討する。一実装では、チャフおよびタグを計算するためのステップは、以下の通りである。

１．チャフと血管の着目点の「比率」パラメータ（例えば、約３．５対４．５）を定義する。

２．キー生成（キータグ）のために使用される各オリジナル点に対してタグ付けされた点を挿入する。

ａ．オリジナル点の場所および記述子情報をその入力として受け取る第１のタグ付け関数を使用して、Ｒ×Ｃウィンドウ内にタグ点を生成する

ｂ．タグ付けされた場所が、オリジナル点のものであるかどうかチェックする

ｉ．該当する場合、何もしない

ｉｉ．該当しないが、１画素半径内にチャフ点が存在する場合、チャフをタグ付けされた場所に移動させる

ｉｉｉ．その他の場合

１．第１のタグ付け関数から生成される場所にチャフ点を作成する

２．最近傍オリジナル点を使用して、前述の点のための記述子を生成する（記述子（ＦｉｎｅＣｈａｆｆＤｅｓｃｒｐｔｏｒ）：）

３．Ｓｅｒｖｅｒ　ＨａｎｄＳｈａｋｅ（ＳｅｒｖｅｒＴａｇ）のために使用される各オリジナル点に対してタグ付けされた点を挿入する。

ａ．第２のタグ付け関数をオリジナル点の場所および記述子情報とともに使用して、Ｒ×Ｃウィンドウ内にタグ点を生成する

ｂ．タグ付けされた点場所が、オリジナル点またはＫｅｙＴａｇであるかどうかチェックする

ｉ．該当する場合、何もしない

ｉｉ．該当しないが、１画素半径内にチャフ点が存在する場合、チャフをタグ付けされた場所に移動させる

ｉｉｉ．その他の場合

１．第２のタグ付け関数から生成される点を作成する

２．最近傍オリジナル点を使用して、前述の点のための記述子を生成する（記述子（ＦｉｎｅＣｈａｆｆＤｅｓｃｒｐｔｏｒ）：）

４．Ｒ×Ｃを等サイズのｋ個のタイルに分割する（例えば、４×５タイルおよびＲ＝８０、Ｃ＝１００、＋／－２０に対しては、ｋ＝２０）。前述の値は、実施例の目的のためのものであり、他の可能な値も考えられることに留意されたい。ある値は、例えば、画像センサ（結果として生じる画像分解能）に基づいて、変化し得る。

５．各タイル内の点の数（Ｏｒｉｇｉｎａｌ＋ＫｅｙＴａｇｓ＋ＳｅｒｖｅｒＴａｇｓ）を計算し、最大（ＭａｘＰｏｉｎｔｓ）を見出す。
６．要求される点を計算し、タイルあたりのタイプを変更する。
ａ．タイル内の点の数が、ＭａｘＰｏｉｎｔｓ／２未満である場合、ＭａｘＰｏｉｎｔｓ／２になるまで、ＣｏａｒｓｅＣｈａｆｆを行い、その後、合計点がＭａｘＰｏｉｎｔｓ＋／－５％に等しくなるまで、ＦｉｎｅＣｈａｆｆを行う。（本例示的アルゴリズムで使用されるように、＋／－Ｘ％は、－Ｘ～＋Ｘの範囲内の乱数を指し得る）
ｂ．タイル内の点の数が、ＭａｘＰｏｉｎｔｓ／２以上の場合、合計点がＭａｘＰｏｉｎｔｓ＋／－５％に等しくなるまで、ＦｉｎｅＣｈａｆｆを行う
７．ステップ６において生成されたチャフのランダムな２０％（より高いチャフカウントに対して増加され得る）に対して、ＣａｆｆＴａｇＣｈａｆｆを作成する。
ａ．第３のタグ付け関数をオリジナル点の場所および記述子情報とともに使用することによって、Ｒ×Ｃウィンドウ内にタグ点を生成する
ｂ．タグ付けされた点場所が、オリジナル点またはＫｅｙＴａｇまたはＳｅｒｖｅｒＴａｇまたはＣｈａｆｆであるかどうかチェックする
ｉ．該当する場合、何もしない
ｉｉ．該当しないが、１画素半径内にチャフ点が存在する場合、チャフをタグ付けされた場所に移動させる
ｉｉｉ．その他の場合
１．第３のタグ付け関数から生成される点を作成する
２．最近傍オリジナル点記述子（ＦｉｎｅＣｈａｆｆＤｅｓｃｒｐｔｏｒ）を使用して、前述の点のための記述子を生成する
８．（ＫｅｙＴａｇ＋ＳｅｒｖｅｒＴａｇ＋ＣｏａｒｓｅＣｈａｆｆ＋ＦｉｎｅＣｈａｆｆ＋ＣａｆｆＴａｇＣｈａｆｆ）／Ｏｒｉｇｉｎａｌ点の数が、比率未満である場合、ＦｉｎｅＣｈａｆｆを作成する。
（ＣｏａｒｓｅＣｈａｆｆ）
１．タイル内に、全点から少なくとも３画素離れたランダムチャフ点を生成する。
２．ＣｏａｒｓｅＣｈａｆｆＤｅｓｃｒｐｔｏｒ：最近傍ＯｒｉｇｉｎａｌＤｅｓｃｒｉｐｔｏｒ（ＯｒｉｇＤｅｓｃ）をとる。
３．ＳＵＲＦ記述子に対して：
ａ．ＮｅｗＳＵＲＦＤｅｓｃｒｐｔｏｒ＝ＣｉｒｃｕｌａｒＳｈｉｆｔ（ＯｒｉｇＤｅｓｃ、＋／－３０％長）＋（０．０１％ガウス雑音）
ｂ．（ＯｒｉｇＤｅｓｃ、ＮｅｗＳＵＲＦＤｅｓｃｒｐｔｏｒ）の正規化されたＳＳＤが、＜０．１の場合、３．ａに進む
４．ＨＬＢＰ記述子に対して：
ａ．ＮｅｗＨＬＢＰＤｅｓｃｒｐｔｏｒ＝ＣｉｒｃｕｌａｒＳｈｉｆｔ（ＯｒｉｇＤｅｓｃ、＋／－３０％長）＋（２０％ガウス雑音）
ｂ．（ＯｒｉｇＤｅｓｃ、ＮｅｗＨＬＢＰＤｅｓｃｒｐｔｏｒ）の正規化されたＳＳＤが、＜０．１である場合、４．ａに進む
５．ＨＤＬＢＰＤｅｓｃｒｐｔｏｒに対して：
ａ．ＮｅｗＨＣＳＬＢＰＤｅｓｃｒｐｔｏｒ＝ＣｉｒｃｕｌａｒＳｈｉｆｔ（ＯｒｉｇＤｅｓｃ、＋／－３０％長）＋（２０％ガウス雑音）
ｂ．（ＯｒｉｇＤｅｓｃ、ＮｅｗＨＣＳＬＢＰＰＤｅｓｃｒｐｔｏｒ）の正規化されたＳＳＤが、＜０．１である場合、５．ａに進む
（ＦｉｎｅＣｈａｆｆ）
１．タイル内に、全点から少なくとも１画素離れたランダム点を生成する。
２．ＦｉｎｅＣｈａｆｆＤｅｓｃｒｐｔｏｒ：最近傍ＯｒｉｇｉｎａｌＤｅｓｃｒｉｐｔｏｒ（ＯｒｉｇＤｅｓｃ）をとる。
３．ＳＵＲＦ記述子に対して：
３．１．ＮｅｗＳＵＲＦＤｅｓｃｒｉｐｔｏｒ＝ＣｉｒｃｕｌａｒＳｈｉｆｔ（Ｏｒｉ

ｇＤｅｓｃ、＋／－３０％長）＋（０．０１％ガウス雑音）
３．２．（ＯｒｉｇＤｅｓｃ、ＮｅｗＳＵＲＦＤｅｓｃｒｉｐｔｏｒ）の正規化されたＳＳＤが、＜０．２である場合、３．１に進む
４．ＨＬＢＰ記述子に対して：
４．１．ＮｅｗＨＬＢＰＤｅｓｃｒｉｐｔｏｒ＝ＣｉｒｃｕｌａｒＳｈｉｆｔ（ＯｒｉｇＤｅｓｃ、＋／－３０％長）＋（２０％ガウス雑音）
４．２．（ＯｒｉｇＤｅｓｃ、ＮｅｗＨＬＢＰＤｅｓｃｒｉｐｔｏｒ）の正規化されたＳＳＤが、＜０．２２５である場合、４．１に進む
５．ＨＤＬＢＰ記述子に対して：
５．１．ＮｅｗＨＣＳＬＢＰＤｅｓｃｒｉｐｔｏｒ＝ＣｉｒｃｕｌａｒＳｈｉｆｔ（ＯｒｉｇＤｅｓｃ、＋／－３０％長）＋（２０％ガウス雑音）
５．２．（ＯｒｉｇＤｅｓｃ、ＮｅｗＨＣＳＬＢＰＤｅｓｃｒｉｐｔｏｒ）の正規化されたＳＳＤが、＜０．２２５である場合、５．１に進む

【００８５】

（ベクトル化関数）

$v_{i,d}$等のスカラーをｋ方向に分割するための単純ではあるが、セキュアかつ効率的方法は、スカラー（または、その関数）をＳＨＡ５１２等のハッシュ関数に提供し、もたらされるビットストリングのグループを所望の一連の数として使用するものである。ベクトル化関数を使用する理由は、以下の通りである。（１）記述子コンテンツ（例えば、それは、特に、特徴ベクトル内のいくつかの場所に対する所与の数値精度の制約内で、ゼロに非常に近くなり得る）にかかわらず、スパンされた線形方程式系の数値安定性、（２）各ベクトル要素が、それ自身の線形混合方程式線にスパンし得るため、複数のまたはより大きいキーコンテンツのためのより大きい容量、および（３）さらなるセキュリティのために、その記憶された値から単に呼び出されるのではなく、方程式係数が、ランタイム時、テンプレート要素によって計算される必要がある。

【００８６】

ベクトル化関数の別の実施例は、以下の通りである。デコードプロセスのための安定した非特異解をもたらす、他の決定論的かつセキュアなベクトル化関数もまた、容認可能である。

【００８７】

疑似乱数生成器（ＰＲＮＧ）に$v_{i,d}$の関数をシードし、ｋ個の疑似乱数の列を作成する。例えば、$f_{md_num_gen}$によって示される暗号法論的にセキュアなＰＲＮＧアルゴリズムを使用して、以下をそれにシードする。

【数１４８】

$$f_{seed}(k, v_{i,d}) = \left\lfloor 2^{31} \left| \cos(k v_{i,d}) \right| \right\rfloor$$

【００８８】

本プロセスにおいて、２つ以上の$v_{i,d}$を使用し、例えば、さらなる数値安定性および不可逆性のために、$v_{i,d} + v_{i,d+1}$（またはそれを上回って、事実上、Ｗの容量の低減を犠牲にして、Ｄを低下させる）を１つに組み合わせることができる。

【００８９】

次に、結果として生じる最初のｋ個の疑似乱数$rnd_seq_{i,i} = 1, 2, \cdots k$をベクトル化された出力としてとる。したがって、ベクトル化関数は、以下となる。

【数１４９】

$$\overrightarrow{rand\_seq}_{i,d} = f_{md\_num\_gen}\left(f_{seed}(k, v_{i,d})\right)$$

【００９０】

随意に、さらなるセキュリティおよびダイナミックレンジ制御のために、前述の$v_{i,d}$スパンベクトルを非自明かつ不可逆的関数φ（χ）に通すことができる。一実施例は、以下の通りである。$md_seq_i = \{rnd_seq_i - 0.5\} \times 8$を適用する（ラ

ンダム列を［－４，４］に線形に投影し、以下の
【数１５０】
$$\varphi(\bullet)$$
を用いてより予測不能な変動をもたらすために）。φ（以下に描写される）に対する一実施例は、以下である。
【数１５１】
$$\varphi(x) = \tanh(x-10)\sin\left((x-10)e^{-\frac{x-10}{2}}\right)$$
【００９１】
最後に、入力$v_{i,d}$のための対応する$y_{i,d}$およびその関連付けられ／エンコードされた
【数１５２】
$$\vec{W}_d$$
（秘密キー行列Ｗの行ｄ）は、以下によって与えられる。
【数１５３】
$$y_{d,i} = f_{encode}\left(\vec{W}_d, v_{d,i}\right) = \sum_{j=1}^{k} w_{d,j}\varphi(rnd\_seq_d(j))$$
前述のように、前述のＳＨＡベースのベクトル化の使用は、これらのタイプのベクトル化の必要性をなくす。
【００９２】
（信頼サーバ機能性）
一実装では、信頼サーバは、局所キーアプローチとともに使用され得る、セキュリティの随意の追加層である。信頼サーバに対する別の追加利点は、サロゲート遠隔確認およびテンプレート／アクセス取り消し可能性である。例えば、サーバが、デバイスによって送信されるトークン（確認時のバイオメトリック眼スキャンマッチングの一意であるが、再発行可能な副産物）を認識しない場合、特定の要求されるトランザクションを受け取るのではなく、信号を、例えば、バイオメトリック認証を使用する当該オンライン銀行業務サービスまたは他のサービスに送信することができる。本実装の詳細は、前述のチャフタグ付けおよびテンプレートマッチングプロセスの大部分と同等である。
【００９３】
【数１５４】
$$T_S: \{\vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d\}, i = 1,2,\ldots,n(T_S) \longrightarrow$$
$$S_{CHF} = H\left(\{\vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d\}\right) = \{h_i\}, i = 1,2,\ldots,n(T_S)$$
の記述子部分のハッシュＨ（．）であるS_{CHF}は、登録時、信頼サーバ上に記録および記憶されるマスタチャフ（例えば、マルチ登録システムにおける登録あたり１つのマスタチャフ記録）として指定されると仮定する。バイオメトリック確認時、信頼サーバ検証が所望される場合、以下の「ハンドシェイク」プロセスが生じ得る。すなわち、テンプレート要素T_{VER}の一致した部分集合が、f_Kに類似するが信頼サーバ機能性のための第２のチャフタグ付け関数f_sに提供され、S_{VER}＝Ｈ（T_{VER}）をもたらし、これは、確認時、信頼サーバに送信される。マッチャの特性から、真正マッチング成功に対して、以下であることが分かっている。
【数１５５】
$$\text{(a)}\ T_{VER} \subset T_{VPD}$$

、および
【数１５６】
$$\text{(b) } n(T_{VER}) \geq k$$
【００９４】
すなわち、マッチ成功は、少なくともｋ個の実血管の着目点を見出し、マッチ失敗（例えば、偽物）は、見出さない。したがって、以下の条件が、デバイス側マッチの完全性を確認するために、サーバ側で満たされる必要があるということになる。
【数１５７】
$$S_{VER} \subset S_{CHF} \text{ および } n(S_{VER}) \geq k$$
【００９５】
例えば、S_{VER}に対するｎ回のＳＨＡ５１２のネスト化反復によって、S_{VER}の時変ハッシュを伝送することもでき、ｎは、汎用タイムスタンプ（例えば、係数）の関数であることに留意されたい。信頼サーバは、任意の比較前に、そのS_{CHF}の同一時変ハッシュを行うであろう。
【００９６】
信頼サーバの他の可能性な機能性は、新しいデバイス上の新しい登録が異なるS_{VER}およびS_{CHF}を作成するであろうため、遠隔サービスへのアクセスの取り消し（例えば、盗難デバイスの場合）を含む。サーバチャフは、キー生成チャフと同じではなく、したがって、この分離は、部分的に独立し、したがって、いくつかの仮説上の攻撃ベクトルにわたるさらなるセキュリティを提供することに留意されたい。それ以外の点では、プライベートキー対サーバチャフの確認正確度および検証セキュリティは、同一と考えられ得る。
【００９７】
初期セキュリティ分析は、以下の通りである。以下のシナリオは、侵害されたデバイスを仮定し、テンプレートは、解読され、バイオメトリック認証コードは、逆コンパイルされ、したがって、デバイス－サーバハンドシェイク論理とテンプレート構造は、攻撃者に既知である。チャフおよび実血管の着目点の判別不能性を前提とすると、テンプレートから最初に当たりくじを引く確率は、以下であるため、せいぜい
【数１５８】
$$\frac{n(T_S)}{n(T_A)}$$
であり、すなわち、テンプレート要素の合計数によって除算される、f_s（（ＶＰＤ）とほぼ同一）別のタグ付けされたチャフの比率である。
【数１５９】
$$P(guess_1 \in T_S, guess_2 \in T_S, \ldots guess_k \in T_S) = \prod_{i=1}^{k} \frac{n(T_S) - i}{n(T_A) - i} < \left(\frac{n(T_S)}{n(T_A)}\right)^k$$
そのような推測は、独立し、同じように分布されることを仮定する。
【００９８】
攻撃者が、推測によって全ての要求される最小ｋ個のT_s元を収集可能な可能性は、極めて低い。各血管の着目点に対して約１つのタグ付けされたチャフ、および各血管の着目点に対して４つの合計挿入チャフの典型的値、および単一２－ＲＯＩスキャンに対するｋ＝４０を使用すると、最初の試みにおける成功の可能性は、以下となる。
【数１６０】
$$\left(\frac{n(T_S)}{n(T_A)}\right)^k = 0.2^{40} = 1.1 \times 10^{-28}$$

信頼サーバが、試みの失敗回数を限定する場合、そのような攻撃に対する成功の全体的可能性は、非常に低いままとなる。さらに、攻撃者が、信頼サーバおよびユーザのデバイスの両方に侵害し、全ての要求されるコンテンツを解読する場合、T_Sは、T_{CHF}の唯一の部分集合であるため、サーバマスタチャフ記録をユーザデバイステンプレートから減算することによって、ユーザテンプレートの血管の着目点部分にアクセスすることができなくなる。

【００９９】

本明細書に採用される用語および表現は、限定ではなく、説明の用語および表現として使用され、そのような用語および表現の使用において、図示および説明される特徴の任意の均等物またはその一部を除外することを意図するものではない。加えて、本開示においてある実装が説明されたが、本明細書に開示される概念を組み込む他の実装も、本発明の精神および範囲から逸脱することなく、使用されることができることが当業者に明白となるであろう。種々の実装の特徴および機能は、種々の組み合わせおよび順列において配列されることができ、全て、開示される発明の範囲内にあると見なされる。故に、説明される実装は、あらゆる点において、制限ではなく、例証であると見なされるものとする。本明細書に説明される構成、材料、および寸法もまた、いかようにも限定として意図されず、例証として意図される。同様に、物理的説明が、説明目的のために提供されたが、任意の特定の理論または機構によって境界される、またはそれに従って請求項を限定するように意図されない。

【図１】

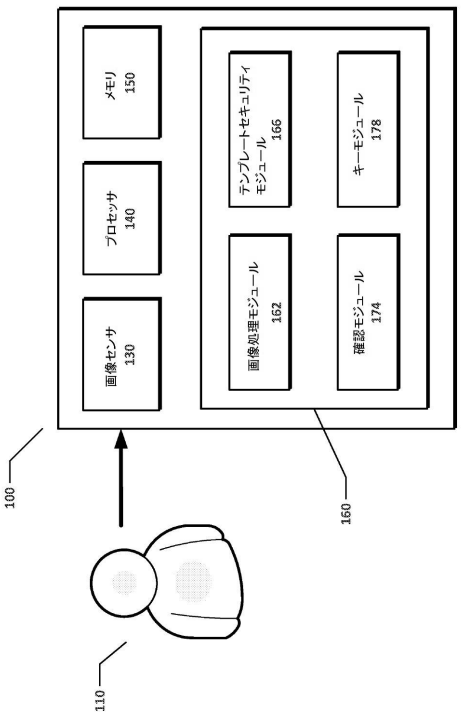

FIG. 1

【図２】

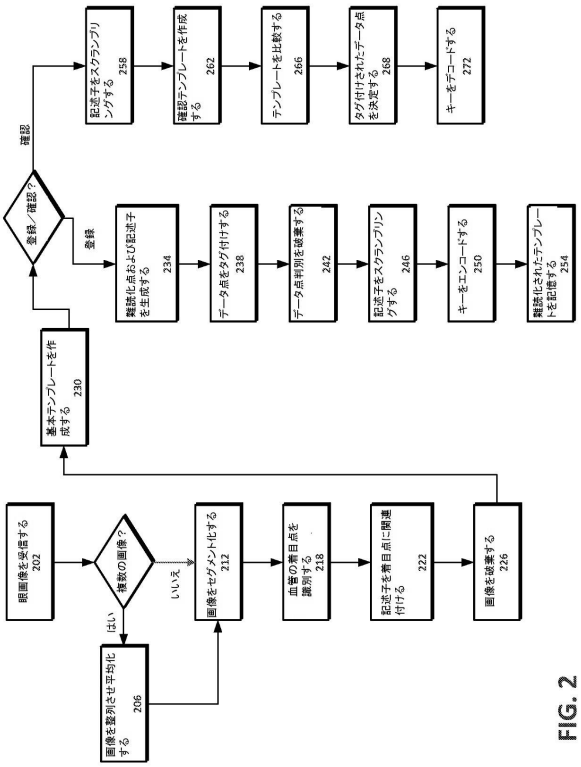

FIG. 2

【図３】

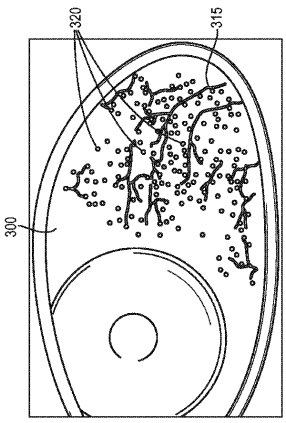

FIG. 3

【図４Ａ】

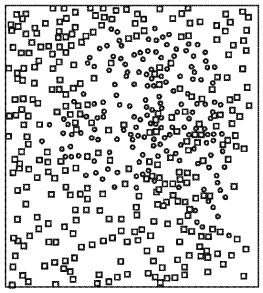

FIG. 4A

【図４Ｂ】

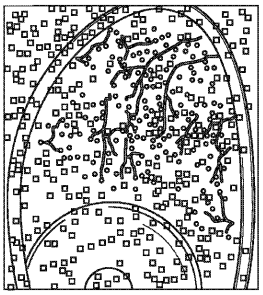

FIG. 4B

【図５】

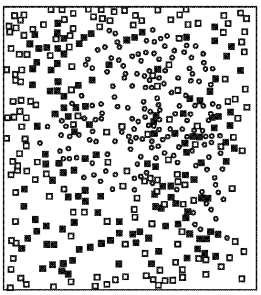

FIG. 5

フロントページの続き

(31)優先権主張番号 14/454,148
(32)優先日 平成26年8月7日(2014.8.7)
(33)優先権主張国 米国(US)

早期審査対象出願

(72)発明者 デラクシャニ, レザ アール.
アメリカ合衆国 カンザス ６６２０５, ロウランド パーク, シダー ストリート ５４４４
(72)発明者 ゴッテムックラ, ビカス
アメリカ合衆国 カンザス ６６１０３, カンザス シティ, ウッドビュー リッジ ドライブ ３１４０, アパートメント ２０５
(72)発明者 サリパッレ, サシ カンス
アメリカ合衆国 カンザス ６６１０３, カンザス シティ, ウッドビュー リッジ ドライブ ３１４０, アパートメント ２０１
(72)発明者 ヒューレット, ケイシー
アメリカ合衆国 カンザス ６６２２７, レネックサ, ウエスト ８６ティーエイチ テラス ２４００３

審査官 新井 則和

(56)参考文献 特表２００７－５００９１０（ＪＰ，Ａ）
特開２０１２－２５６２７２（ＪＰ，Ａ）
特開２００９－０２６２３５（ＪＰ，Ａ）
特開２０１１－０１３９１２（ＪＰ，Ａ）
米国特許出願公開第２００２／０１２０５９２（ＵＳ，Ａ１）
米国特許出願公開第２０１１／０１２３０７２（ＵＳ，Ａ１）
大木 哲史 外3名, Ｆｕｚｚｙ Ｆｉｎｇｅｒｐｒｉｎｔ Ｖａｕｌｔ Ｓｃｈｅｍｅによるバイオメトリック暗号のロック情報作成手法, 情報処理学会論文誌 論文誌ジャーナル Ｖｏｌ．５０ Ｎｏ．９ ［ＣＤ－ＲＯＭ］ 情報処理学会論文誌 Ｖｏｌ．５０ Ｎｏ．９, 日本, 社団法人情報処理学会, ２００９年 ９月１５日, Ｖｏｌ．５０ Ｎｏ．９, pp. 2077-2087, ISSN 1882-7837

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｔ １／００
Ｇ０６Ｔ ７／００
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／３２
Ｇ０６Ｆ ２１／６０