

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4601703号
(P4601703)

(45) 発行日 平成22年12月22日 (2010.12.22)

(24) 登録日 平成22年10月8日 (2010.10.8)

(51) Int. Cl.	F I
G 0 6 F 7/58 (2006.01)	G O 6 F 7/58 A
G 0 9 C 1/00 (2006.01)	G O 9 C 1/00 6 5 O B

請求項の数 30 (全 17 頁)

(21) 出願番号	特願2008-502991 (P2008-502991)	(73) 特許権者	505425317
(86) (22) 出願日	平成18年2月22日 (2006.2.22)		ダウ コーニング コーポレイション
(65) 公表番号	特表2008-537622 (P2008-537622A)		アメリカ合衆国 4 8 6 8 6 - 0 9 9
(43) 公表日	平成20年9月18日 (2008.9.18)		4 ミシガン、ミッドランド、ウエスト
(86) 国際出願番号	PCT/US2006/006029		ザルツブルク ロード 2 2 0 0、ピ
(87) 国際公開番号	W02006/101645		ー、オー、ボックス 9 9 4
(87) 国際公開日	平成18年9月28日 (2006.9.28)	(74) 代理人	100066692
審査請求日	平成20年11月14日 (2008.11.14)		弁理士 浅村 皓
(31) 優先権主張番号	60/664, 307	(74) 代理人	100072040
(32) 優先日	平成17年3月21日 (2005.3.21)		弁理士 浅村 肇
(33) 優先権主張国	米国 (US)	(74) 代理人	100091339
			弁理士 清水 邦明
		(74) 代理人	100094673
			弁理士 林 拓三

最終頁に続く

(54) 【発明の名称】 散乱導波管を使用した乱数の発生技術

(57) 【特許請求の範囲】

【請求項 1】

コヒーレント光を発生するための光源と、
前記コヒーレント光を受け、散乱光を発生するための散乱導波管とを備え、
前記光源と前記散乱導波管の相対的位置は可変であり、
更に散乱光に基づき少なくとも1つの乱数を形成するための検出器を備える装置。

【請求項 2】

前記光源は、レーザーを含む、請求項 1 記載の装置。

【請求項 3】

前記光源と前記散乱導波管との間に配置された端面カップリング、回折格子カップリングおよびプリズムカップリングのうちの少なくとも1つを含む、請求項 2 記載の装置。 10

【請求項 4】

前記散乱導波管は、単一モードのプレーナー状導波管を含む、請求項 1 記載の装置。

【請求項 5】

前記単一モードのプレーナー状導波管は、
第 1 クラッド層と、
前記第 1 クラッド層の上方に形成された第 1 コア層と、
前記第 1 コア層の上方に形成された第 2 クラッド層とを備える、請求項 4 記載の装置。

【請求項 6】

前記第 1 コア層内に形成された複数の散乱ピラーを備える、請求項 5 記載の装置。 20

【請求項 7】

前記散乱ピラーと、前記第 1 および第 2 クラッド層とは、同じ材料から構成されている、請求項 6 記載の装置。

【請求項 8】

前記第 1 クラッド層および前記第 2 クラッド層は前記コア層の屈折率に対して選択された屈折率の比を有する、請求項 6 記載の装置。

【請求項 9】

前記導波管の温度を制御することによって、前記コアおよび前記クラッド層の屈折率を調節できる、請求項 7 記載の装置。

【請求項 10】

前記導波管を横断する電界を変えることにより、前記コア層の屈折率を調節できる、請求項 7 記載の装置。

【請求項 11】

前記散乱導波管は、テクスチャー状の側壁を有するフレア導波管を備える、請求項 1 記載の装置。

【請求項 12】

前記散乱導波管に入射する光の角度を変えることができる、請求項 1 記載の装置。

【請求項 13】

前記光源および散乱導波管の直線方向の相対的位置を変えることができる、請求項 1 記載の装置。

【請求項 14】

6 までの運動自由度を有する複数の運動光学的マウントを備える、請求項 1 記載の装置。

【請求項 15】

前記検出器は、CCDカメラおよびフォトダイオードアレイのうちの少なくとも 1 つを含む、請求項 1 記載の装置。

【請求項 16】

前記検出器は、前記 CCDカメラまたはフォトダイオードアレイによって捕捉された画像を示す情報にアクセスするための画像プロセッサを含む、請求項 15 記載の装置。

【請求項 17】

前記画像プロセッサは、前記 CCDカメラまたはフォトダイオードアレイによって捕捉された画像を示す情報に基づき乱数を形成する、請求項 16 記載の装置。

【請求項 18】

光源と散乱導波管との相対的位置を選択するステップと、
前記光源を使用して前記散乱導波管にコヒーレント光を提供するステップと、
前記散乱導波管によって散乱された光を受けるステップと、
前記散乱された光に基づき乱数を形成するステップとを備えた方法。

【請求項 19】

相対的位置を選択する前記ステップは、前記散乱導波管の回転位置を選択することを含む、請求項 18 記載の方法。

【請求項 20】

相対的位置を選択する前記ステップは、前記光源と前記散乱導波管との相対角方向の配置を選択することを含む、請求項 18 記載の方法。

【請求項 21】

相対的位置を選択する前記ステップは、前記光源と前記散乱導波管の端面との相対角方向の配置を選択することを含む、請求項 18 記載の方法。

【請求項 22】

相対的位置を選択する前記ステップは、前記光源および前記散乱導波管の直線方向の相対的位置を選択することを含む、請求項 18 記載の方法。

【請求項 23】

コヒーレント光を提供する前記ステップは、レーザーを使用してコヒーレント光を発生することを含む、請求項 18 記載の方法。

【請求項 24】

コヒーレント光を受ける前記ステップは、端面カップリング、回折格子カップリングおよびプリズムカップリングのうちの少なくとも 1 つを介してコヒーレント光を受けることを含む、請求項 18 記載の方法。

【請求項 25】

コヒーレント光を受ける前記ステップは、複数の散乱ピラーを含む散乱導波管を使用してコヒーレント光を受けることを含む、請求項 18 記載の方法。

【請求項 26】

コヒーレント光を受ける前記ステップは、テクスチャー状の側壁を有するフレア状導波管を含む散乱導波管を使用してコヒーレント光を受けることを含む、請求項 18 記載の方法。

【請求項 27】

コヒーレント光を受ける前記ステップは、CCDカメラまたはフォトダイオードアレイのうちの少なくとも 1 つを使用してコヒーレント光を受けることを含む、請求項 18 記載の方法。

【請求項 28】

乱数を形成する前記ステップは、前記 CCDカメラまたは前記フォトダイオードアレイによって捕捉された画像を示す情報にアクセスすることを含む、請求項 27 記載の方法。

【請求項 29】

乱数を形成する前記ステップは、前記 CCDカメラまたは前記フォトダイオードアレイによって捕捉された画像を示す情報に基づき乱数を形成することを含む、請求項 28 記載の方法。

【請求項 30】

光源と散乱導波管との相対的位置を選択する手段と、
前記光源を使用して前記散乱導波管にコヒーレント光を提供する手段と、
前記選択された場所の散乱導波管によって散乱された光を受ける手段と、
前記散乱された光に基づき乱数を形成する手段とを備えた装置。

【発明の詳細な説明】

【技術分野】

【0001】

(発明の背景)

(1. 発明の分野)

本発明は、一般的にはデータの暗号化に関し、より詳細には、散乱導波管を使用した乱数の発生技術に関する。

【背景技術】

【0002】

(2. 関連技術の説明)

インターネット、ワールドワイドウェブならびに安全な政府イントラネットおよび会社のイントラネットを含む種々のイントラネットを含む最近の通信ネットワークは、ネットワークと通信できる実質的に任意のデバイスに大量のデータを送信できる。政府機関、工業および商業的事業所および個人としての市民は、安全かつ効率的にデータを送信するためにこれらネットワークに頼るようになった。例えば個人としての市民は、インターネットを通して個人情報およびクレジットカードの情報を提供することにより、種々の商業的事業所に製品およびサービスを注文できる。個人としての市民および商業的事業所の双方は、第三者によって情報が盗まれないよう、この情報を安全に送信することをネットワークに頼っている。別の例として、政府機関は、機関の間のイントラネットを使って秘密文書を送信するであろう。従って、政府機関は文書の秘密を保持することを、これら通信ネットワークに頼っている。従って、種々の通信ネットワークを通して送信される情報は—

10

20

30

40

50

般に暗号化される。

【発明の開示】

【発明が解決しようとする課題】

【0003】

暗号化鍵を使ってデータを暗号化することが可能である。例えば公開鍵暗号化では、ユーザーはユーザーにしか知らないはずのプライベート暗号化鍵および誰にも利用できる公開鍵を使用する。ユーザーが送ったデータは、公開鍵および計算関数、例えばハッシング関数を使って暗号化できる。この暗号化されたデータは、プライベート鍵にアクセスできる者にしか解読できない。ユーザーがプライベート鍵を秘密に維持している限り、公開鍵を使って暗号化されたデータは、どの人またはエンティティにとっても解読は禁止的に不可能である。しかしながら、単一のプライベート鍵の値は、比較的容易に決定できる。例えばプライベート鍵が記載されたポストイットノートを詳細に検討することにより、安全性が保たれていないロケーションなどからコンピュータに記憶されているプライベート鍵に直接または遠隔的にアクセスすることにより、あるいは同様のことによりプライベート鍵の値を決定できる。

10

【0004】

従って、安全情報を定期的に送信したり、または高度に機密状態の情報を送信したりするユーザーまたは機関は、乱数の暗号化鍵発生器を使用し、定期的に新しい暗号化鍵を提供できる。暗号化鍵を発生するのに使用される計算関数は、一般に簡潔であり、当業者には周知であることが多い。従って、暗号化されたデータに対する攻撃が成功することにより、または内部情報を使用して限られた数の鍵が発見された場合、巧妙な敵対者は将来の暗号化鍵を予測できる。このようなタイプの攻撃は、一般に公知鍵の攻撃と称されている。暗号化鍵発生器のセキュリティを密かに低下させるには、妥協した単一の暗号化鍵で十分であるケースもある。

20

【0005】

本発明は、上記問題の1つ以上の影響を解決せんとするものである。

【課題を解決するための手段】

【0006】

(発明の概要)

次の説明は、本発明の一部の特徴を基本的に理解できるようにするために、本発明の簡略化された概要を示すものである。この概要は、本発明の消尽的な概観ではなく、本発明のキーとなる要素またはクリティカルな要素を識別したり、発明の範囲を定めたりするためのものではない。この説明の単一の目的は、後述するより詳細な説明に対する序文として、一部の原理を簡略的な形態で示すことにある。

30

【0007】

本発明の一実施例では、散乱導波管を使用した乱数発生のための装置が提供される。この装置は、コヒーレント光を発生するための光源と、このコヒーレント光を受け、散乱光を発生するための散乱導波管とを備える。光源と散乱導波管との相対的な位置を変えることができ、この装置は、散乱光に基づき、少なくとも1つの乱数を発生するための検出器も含む。

40

【0008】

本発明の一実施例では、散乱導波管を使って乱数を発生するための方法が提供される。この方法は、光源と散乱導波管との相対的な位置を選択するステップと、光源を使ってコヒーレント光を散乱導波管に提供するステップと、選択された位置にある散乱導波管により散乱された光を受けるステップと、散乱光に基づいて乱数を形成するステップとを含む。

【0009】

添付図面と関連をとった次の説明から本発明について理解できよう。図中、参照番号は同様な要素を示す。

【0010】

本発明は、種々に変形したり、別の形態にしたりし易いが、図面には本発明の特定の実

50

施例を例として示し、明細書では詳細に説明した。しかしながら、特定の実施例の本明細書の説明は、開示する特定の形態に本発明を限定するものではなく、むしろ逆に本発明は特許請求の範囲に記載した発明の要旨に入るすべての変形例、均等物および代替例をカバーするものであると理解すべきである。

【実施例】

【0011】

次に、本発明の図示する実施例について説明する。明瞭にするために、本明細書では実際の実現例のすべての特徴事項について説明するわけではない。当然ながら、かかる実際の実施例を開発するに当たり、開発者の特定の目標、例えば実現例ごとにより変り得るシステムおよび業務に関連する制限とのコンプライアンスを達成するために、実現例固有の多数の判断を行っていることが理解できよう。更に、かかる開発努力は複雑で、かつ時間のかかることであるが、本明細書の開示に利益を有する当業者にとってルーチン作業ではないと理解できよう。

【0012】

コンピュータメモリ内のデータビットでのオペレーションのソフトウェアまたはアルゴリズム、およびシンボル表示として、本発明の一部および対応する詳細な説明を示す。当業者は他の当業者に作業の実態を効果的に伝えるためにこれら説明および表示を、使用するものである。本明細書において、用語を使用し、一般的に使用する際のアルゴリズムは、所望する結果を生じさせる自己完結的シーケンスのステップであると見なされる。これらステップは、物理的な量を物理的に操作することを必要とするステップである。通常、これら量は、記憶し、転送し、組み合わせ、比較し、他の方法で操作することができる光学的、電氣的または磁氣的信号の形態をとり得るが、必ずしもこのような形態でなくてもよい。主に、共通に使用する理由からこれら信号をビット、値、要素、シンボル、キャラクター、ターム、番号等と称することがときどき便利であることが証明されている。

【0013】

しかしながら、これらの同様な用語のすべては、適当な物理的な量と関連付けすべきであり、単にこれら量に対して使用される適当な表示にすぎないことを念頭に入れるべきである。特に、別に表記しない限り、または本明細書から明らかなように、「処理」または「コンピューティング」または「計算」または「決定」または「ディスプレイ」などの用語は、コンピュータシステムのレジスタおよびメモリ内の物理的、電子的量として表示されたデータを操作し、これらデータをコンピュータシステムのメモリまたはレジスタ、もしくははかかる他の情報記憶デバイス、送信デバイスまたはディスプレイデバイス内の物理的量として同様に表示される他のデータに変換するコンピュータシステムまたは同様な電子計算デバイスの作用およびプロセスを示す。

【0014】

本発明のソフトウェアによって実行される特徴は、一般に、ある形態のプログラム記憶媒体上でコード化されるか、またはあるタイプの送信媒体を通して実施されることにも留意されたい。プログラム記憶媒体は磁気（すなわちフロッピー（登録商標）ディスクまたはハードドライブ）または光学的（例えばコンパクトディスク、リードオンリーメモリまたはCD ROM）でもよいし、読み取り専用またはランダムアクセスするようなものでもよい。同様に、送信媒体は、撚り対線、同軸ケーブル、光ファイバーまたは当業者に公知の他の適当な送信媒体でもよい。本発明は、所定の実施例のこれら特徴によって限定されるものではない。

【0015】

以下、添付図面を参照し、本発明について説明する。説明する目的のためだけに、かつ当業者に周知の細部により、本発明を不明瞭にしないように、種々の構造、システムおよびデバイスを図面に略図として示した。それにもかかわらず、本発明の図示した例を記述し説明するために、添付図面が含まれる。本明細書で使用する単語およびフレーズは、当業者によるこれら単語およびフレーズの理解と一致する意味を有すると理解し、解釈すべきである。用語またはフレーズの特殊でない定義、すなわち当業者が理解するような通常

または習慣的な意味とは異なる定義は、本明細書の用語およびフレーズの一貫した使用によって意味されるものである。特別な意味、すなわち当業者が理解する以外の意味を用語またはフレーズが有する程度に、この用語またはフレーズに対する特別な定義を直接かつ非同義的に提供する一定の態様で、本明細書に明らかに記載する。

【0016】

次に図1を参照すると、ここには、乱数、例えばランダムな暗号化鍵を発生するためのシステム100が示されている。このシステムは光源105を含み、図示された実施例では、光源105はレーザーである。例えば光源105は従来のデスクトップレーザー、例えば633nmのHeNeレーザーとすることができる。しかしながら、当業者であれば、本発明は従来のデスクトップレーザーだけに限定されないことが理解できるはずである。別の実施例では、任意の望ましいタイプのレーザーを使用できる。例えば光源105は、所望するガス活性媒体を使用して形成される望ましい特性波長を有するレーザーとすることができ、システム100を半導体デバイスの一部として実施するとき使用できる別の例のために、光源105を半導体ダイオードレーザーとすることができる。このシステム100は、他の要素、例えばミラー、レンズ、フィルタ、回折格子および図1に示されていない同様なものも含むことができる。

【0017】

光源105は、矢印110が示すように、散乱導波管115にコヒーレント光を供給する。当業者であれば、光源105が発するコヒーレント光110は、無限距離にわたって完全にコヒーレントでなくてもよいと理解できるはずである。その代わりに当技術分野の一般的な使用によれば、「コヒーレント」なる用語はシステム100に関連する1つ以上の特性長さスケールと同じオーダー、またはそれ以上の長さスケールにわたってコヒーレントである光を意味する。例えばこのコヒーレント光110は、散乱導波管115に関連する長さスケール、例えば散乱導波管115の高さ、太さおよび/または長さ少なくとも同じである長さスケールにわたってコヒーレントであればよい。従来の633mmのHeNeレーザーは、約1mのコヒーレント長さを有することができ、半導体ダイオードレーザーは約1cmのコヒーレント長さを有することができる。図示された実施例では、エンドフェースカップリング120を介し、散乱導波管115にコヒーレント光110が提供される。例えばエンドフェースカップリング120は、ビームが(例えば散乱導波管115の太さに基づく)適当なスポットサイズおよび/または(例えば散乱導波管115の屈折率および屈折率の比によって決定される)開口数を有するように、コヒーレント光110の形状を定める1つ以上のレンズを含むことができる。一実施例では、端面カップリング120は、散乱導波管115のガイドレジーム内で発射される光量を増加できる。

【0018】

光源105に対する散乱導波管115の位置を変えることができる。図示された実施例では、散乱導波管115は散乱導波管115の直線方向の位置を変えることができるようにする第1可動光学的マウント125に取り付けられている。例えば散乱導波管115は、コヒーレント光110の伝搬方向に垂直な方向に移動できる。散乱導波管115の図示された実施例も、散乱導波管115の回転角方向の向きを変えることができるようにする第2可動光学的マウント130に取り付けられている。例えばこの散乱導波管は、図1の平面に対して垂直な軸線を中心として回転できる。第1可動光学的マウント125と第2可動光学的マウント130は、6つの運動自由度を有し、これによって散乱導波管115のリニアな向きおよび/または回転角方向の向きを完全に制御することが可能となっている。詳細に後述するように、散乱導波管115の直線方向の位置を変えることによってシステム100により、複数の乱数暗号化鍵を発生することが可能となっている。

【0019】

散乱導波管115は、複数の散乱サイト(図1には示されず)を含み、これらサイトは散乱導波管115の一部にわたってランダムに分布できる。従って、矢印135が示すように、散乱光を形成するために、散乱導波管115内でコヒーレント光110を散乱できる。散乱光135の少なくとも一部が検出器140に入射できる。種々の別の実施例では

、検出器 140 は CCD カメラ、フォトダイオードアレイおよび同等物とすることができ、詳細に後述するように、検出器 140 は画像プロセッサ 145 に散乱光 135 の複数の強度を示す信号を提供でき、プロセッサ 145 は、散乱光 135 の複数の強度を示す信号に基づき、乱数を発生できる。この乱数を乱数暗号化鍵として使用できる。

【0020】

図 2 A および 2 B は、散乱導波管 200 の第 1 実施例の側面図および平面図をそれぞれ概念的に示す。散乱導波管 200 の第 1 実施例は、第 1 クラッド層 205 と、第 1 コア層 210 と、第 2 クラッド層 215 とを含む。しかしながら当業者であれば、散乱導波管 200 はこれら層だけに限定されないことが理解できるはずである。別の実施例は、上記よりも多いかそれよりも少ない層を含むことができる。例えば第 1 クラッド層 205 を基板（図示せず）に形成でき、一実施例では、第 1 および第 2 クラッド層 205、215 および第 1 コア層 210 はエポキシ官能化シロキサン樹脂から形成された単一モードの平面状導波管の一部である。しかしながら、別の実施例では、層 205、210、215 を形成するために望ましい任意の材料を使用できる。

【0021】

第 1 コア層 210 内には複数の散乱ピラー 220 が形成されており、図示された実施例では、これら散乱ピラー 220 は第 1 クラッド層 205 および第 2 クラッド層 215 を形成するのに使用された材料と同じ材料から形成されている。例えば散乱ピラー 220 は、エポキシ官能化シロキサン樹脂から形成できる。散乱ピラー 220、第 1 クラッド層 205 および第 2 クラッド層 215 は、約 1.0 % の第 1 コア層 210 を形成するのに使用された材料と対照的な屈折率を有する。しかしながら、別の実施例では、散乱ピラー 220 は任意の望ましい材料から形成でき、所望する屈折率の比を有することができる。当業者であれば、層 205、210、215 の厚さは、選択された屈折率の比によって影響され得ることが理解できるはずである。

【0022】

上記とは異なり、導波管 200 は屈折率および屈折率の比を制御できる態様で変更できるようにする光学的材料から構成できる。この変更は永久的でもよいし、リバーシブルでもよい。かかる変更に至るルートは、熱光学的チューニング、電気光学的効果、カー効果、物理的歪みまたは応力、もしくは導波管材料による追加化学的種の吸収を含むが、これらだけに限定されるものではない。例えば感温性材料の温度を調節すると、屈折率が変

【0023】

図示された 2 B に示される散乱ピラー 220 は、横断面が円形である。一実施例では、散乱ピラー 220 の直径は、約 200 ミクロンでよい。633 nm の HeNe レーザーと共に散乱導波管 200 の図示された実施例を使用する場合、散乱ピラー 220 の特性長さスケールは、コヒーレント光の波長よりも大きくなる。従って、コヒーレント光は、圧倒的に前方方向に散乱される。すなわち、コヒーレント光は、圧倒的に Mie 散乱される。しかしながら、当業者であれば、本発明は、200 ミクロンの直径を有し、横断面が円形の散乱ピラーだけに限定されないことが理解できるはずである。別の実施例では、散乱ピラー 220 は、任意の望ましい横断面の形状および/または寸法を有することができる。さらに散乱ピラー 220 の寸法および/または横断面の形状は、ある値のレンジにわたって分散してよい。

【0024】

図 3 は、散乱ピラー 220 の第 2 実施例を概念的に示す。図示された実施例では、散乱導波管 300 は、導波管領域 305 と送信領域 310 とを含む。導波管領域 305 と送信領域 310 とは、任意の望ましい材料から形成できる。例えば、導波管領域 305 と送信領域 310 とは、エポキシ官能化シロキサン樹脂から形成できる。導波管領域 305 の屈折率と昇進領域 310 の屈折率は、所定の値だけ異なる。例えば導波管領域 305 の屈折

率と送信領域 310 の屈折率の比は、約 1.0 % である。しかしながら、当業者であればこの屈折率の比は設計上の事項に過ぎず、実施例が異なれば、変わってもよいことが理解できるはずである。

【0025】

送信領域 310 の側壁 315 は、特徴部 320 が示すように、テクスチャー状となっている。当業者であれば、このテクスチャー状特徴部 210 は側壁 315 に沿って任意の望ましい形状および/または分布となってもよいことが理解できるはずである。一実施例では、テクスチャー状特徴部 320 の特性長さのスケールは、散乱導波管 300 に入力されるコヒーレント光の波長よりも大きくなるように選択されている。この実施例では、前方の Mie 散乱が圧倒的である。側壁 315 のフレアはコヒーレント光が散乱導波管 300 によって送信および/または散乱されたときに形成される干渉パターンにおける別の複雑な構造となる側壁 315 のテクスチャー状により、ガイドされた光のモードによる分岐を生じさせ得る。従って、散乱光の分布はコヒーレント光のコヒーレント長さにあまり影響されないので、モデル化がより容易である。しかしながら、散乱導波管 300 を使って形成される暗号化鍵は図 2A ~ B に示される散乱導波管 200 を使って形成される暗号化鍵よりも多少安全性が低くなり得る。

【0026】

図 4 は、画像捕捉および処理システム 400 の一実施例を概念的に示す。この図示された実施例では、画像捕捉および処理システム 400 は光検出器 405 を含む。例えばこの光検出器 405 は CCD 検出器、すなわちカメラ、フォトダイオードアレイなどでよい。光検出器 405 は上部に複数の感光性素子 410 が分布した表面を有する。例えば CCD 検出器は複数の電荷結合デバイスを含み、フォトダイオードアレイは複数の感光ダイオードを含むことができる。光検出素子 410 を本明細書ではピクセル 410 と称す。各ピクセル 410 は、ピクセル 410 に入射、またはその近くに入射する光の強度を示す信号を発生できる。

【0027】

1 つ以上のピクセル 410 に、またはその近くに入射する光の強度を示す信号の 1 つ以上に、画像捕捉モジュール 415 がアクセスできる。一実施例では、画像捕捉モジュール 415 は、点線のボックス 420 が示すように、選択された複数のピクセル 410 が発生する信号にアクセスする。例えば光検出器 405 が 720 ピクセル × 480 ピクセルの寸法を有する CCD カメラである場合、画像捕捉モジュール 415 は 512 ピクセル × 50 ピクセルの寸法を有するサブセット 420 からの情報にアクセスできる。次に画像捕捉モジュール 415 は選択されたサブセット 420 内のピクセル 410 が提供する強度情報に基づき、強度 430 のプロット 425 を形成する。例えば強度 430 は、サブセット 420 の 512 秒の各々における 50 個のピクセルにわたって平均化された 512 個の強度に対応する 512 個の強度の値を含むことができる。

【0028】

一実施例では、画像プロセッサ 435 は、強度 430 に基づき、乱数を形成する。例えば画像プロセッサ 435 は、512 個の強度と、乱数 445 の 512 バイト 440 とを関連付けできる。次にビット 440 のうちの 1 つに関連した強度がスレッシュホールド 450 よりも低ければ、ビット 440 の値を「0」にセットし、ビット 440 に関連する強度がスレッシュホールド 450 よりも大きければ、ビット 440 の値を「1」にセットする。当業者であれば、このスレッシュホールドの値は、設計事項にすぎないことが理解できるはずである。更に本発明は、スレッシュホールドを使った乱数 445 の決定だけに限定されない。別の実施例では、検出器 405 が検出した光に基づき、所望する態様で乱数 445 を形成できる。512 個のバイトを含む実施例では、 10^7 の数よりも多い乱数スペースを単一のデバイスによってカバーできる。

【0029】

検出器 405、画像捕捉モジュール 415 および画像プロセッサ 435 は、図 4 に示された画像捕捉および処理システム 400 内の別個の要素として示されているが、当業者で

10

20

30

40

50

あれば本発明はこのように限定されないことが理解できるはずである。別の実施例では、検出器405、画像捕捉モジュール415および画像プロセッサ435は、それ以上多いか、少ない、別個の要素として構成できる。更に画像捕捉および処理システム400内には、図を明瞭にするため、図4には示されていない別の要素を含むことができる。当業者であれば、別の実施例は、検出器405、画像捕捉モジュール415および画像プロセッサ435の一部を、ソフトウェア、ファームウェア、ハードウェアまたはそれらの組み合わせで実現できることが理解できるはずである。例えば画像捕捉および処理システム400は、LabVIEW(登録商標)画像捕捉および処理アルゴリズムを実現するソフトウェアを含むことができる。

【0030】

10

図5は、散乱光に基づき、乱数を形成する方法500の一実施例を概念的に示す。図示されている実施例では、散乱導波管の配置が(505で)選択されている。一実施例では、散乱導波管の直線方向および/または回転角方向の配置を制御するのに可動光学的マウントを使用できる。例えば散乱導波システムが633nmのコヒーレント光を使用している場合、散乱導波管を少なくとも10マイクロラジアンだけ回転することによって乱数を発生できる。これとは異なり、約5~10ミクロンだけ、入射コヒーレント光の伝搬方向を横断するように散乱導波管を変位させてもよい。

【0031】

(510)にて散乱導波管にコヒーレント光を与え、散乱導波管によって散乱された光に(515で)アクセスする。例えばレーザーによって(510で)コヒーレント光を提供し、上で詳細に説明したように、CCD検出器またはフォトダイオードアレイのような検出器を使って(515で)散乱光にアクセスできる。アクセスした散乱光に基づき(520で)乱数暗号化鍵のような乱数を形成する。当業者であれば、(520で)形成される乱数を、例えば相互相関化尺度または相対的エントロピー尺度によって形成されるような統計的意味におけるランダムと見なすことができると理解できるはずである。

20

【0032】

上記本発明の実施例を使用して形成された乱数暗号化鍵のような乱数は、乱数を形成するための従来技術よりも多数の利点を有することができる。乱数発生システムの物理的作動パラメータ、例えばコヒーレント光の入射角、コヒーレント光の波長などを変えることにより、多くの暗号化鍵を定めるのに、単一の散乱導波管を使用できる。散乱導波管に基づく乱数発生用システムは、多数の散乱のカスケード特性に起因し、本来的に反転できないものでもある。従って、公知の鍵への攻撃の危険性を解消または低減できるよう、散乱導波管の構造をリバースエンジニアリングすることが極めて困難または不可能である。このように発生された暗号化鍵は、現在の通信インフラストラクチャにおいて使用される対照的な鍵暗号化方式にも適している。更に、意図する用途に応じて散乱サイトが同じように分布する大きいファミリーの導波管または単一のユニークなパターン化されたデバイスを製造できる。

30

【0033】

散乱導波管の構造に対する多重散乱の感受性によって、別の暗号化鍵セキュリティを提供できる。例えば最小限の物理的な不正操作でも、デバイスの性能を大幅に変え、デバイスを効果的に破壊し、デバイスを通信ネットワークから外し得る。更に、要求時に乱数暗号化鍵を発生し、アクティブなメモリに暗号化鍵を記憶する必要性を解消または低減できる。アクティブメモリ内に乱数暗号化鍵を発生する技術を表示する情報を記憶する必要性も低減できる。従って、敵対者がこの情報にアクセスする可能性も低減できる。

40

【0034】

図6~8は、ガイド層にわたって散乱ピラーがランダムに分散されたスラブ導波管を含む乱数発生器の一実施例の作動を概念的に示す。当業者であれば、図6~8を参照して説明した実施例は、本発明を説明するためのものであり、本発明を限定するものではないと理解できるはずである。

【0035】

50

図 6 A および 6 B は、単結晶シリコン基板に構成された対称的なポリマー製のスラブ導波管の一実施例を概念的に示す。図 6 A は、導波管の広角図を示し、図 6 B は、導波管のクローズアップ図を示す。導波管はコア層 6 1 5 内に形成された、ランダムに分散された複数の散乱ピラー 6 1 0 を備える。図示された実施例では、導波管のクラッド層（図示せず）およびコア層 6 1 5 は、ダウコーニング社の光パターン化可能な光学的材料 OE 5 9 9 3（低屈折率）および OE 5 9 9 3（高屈折率）からそれぞれ形成されている。ここで、OE 5 9 9 3 の低屈折率組成物は、光学的希釈剤を含む。導波管の各層を、逐次スピンコーティングし、Q u i n t e l Q - 7 0 0 0 マスクアライナーを使って（必要に応じて）パターン化し、ウェットエッチングプロセスで現像する。クラッド層、すなわち OE 5 9 9 3（低屈折率）は、 $n = 1.51$ の屈折率および約 $20 \mu\text{m}$ の厚みを有する。コア層、すなわち OE 5 9 9 3（高屈折率）は、 $n = 1.53$ の屈折率および約 $2 \sim 4 \mu\text{m}$ の厚みを有する。コア層 6 1 5 内の散乱ピラー 6 2 0 の材料は、クラッド層と同じである。

【 0 0 3 6 】

図 6 A ~ B に示される散乱ピラー 6 1 0 を形成するために、ベンチマークテクノロジー社による仕様に従って製造されたリソグラフィーマスクカスタムを使って感光性ポリマー内に円形ビアをパターン形成し、次にコア材料からエッチングする。これらビアをクラッド材料 OE 6 0 6 1 でバックフィルし、頂部クラッド層をスピンコーティングし、構造全体をプレナー状にする。

【 0 0 3 7 】

個々の散乱導波管はサイズが $1 \text{ cm} \times 1 \text{ cm}$ であり、各導波管は約 6 5 0 本の散乱ピラー 6 1 0 を含む。導波管のコア層 6 1 5 内にパターン形成された 6 5 0 本の散乱ピラー 6 1 0 の分布および寸法は、所定のパラメータ値内に正常にランダムに分布している。これらピラーの直径は $250 \sim 350 \mu\text{m}$ の範囲であった。ピラー位置の中心はピラーのエッジが理節するピラーのエッジおよびデバイスのエッジから最低 $5 \mu\text{m}$ となるように限定された。ダイヤモンドのこぎりを使って個々に $1 \text{ cm} \times 1 \text{ cm}$ の散乱導波管をダイシングし、エンド面で 8° の角度の光学的仕上げとなるように研磨した。

【 0 0 3 8 】

これら導波管は 632.8 nm で作動するヘリウム - ネオンレーザーを使用することを特徴としていた。光学的 - 機械式マウントに導波管を取り付け、組み合わせで自由度を 6 にし、サンプルを照射するようにヘリウム - ネオンレーザーを使用した。導波管の開口数にほぼ一致する 0.25 の開口数を有する 10 倍の顕微鏡用対物レンズを使用し、レーザーからのコリメート化された光を導波管に端面結合した。ワーテック社の W A T - 2 0 2 B C C D カメラおよびイメージプロプラスの $4.5.1$ ソフトウェアを用いて、導波管から出た散乱光の画像を形成した。

【 0 0 3 9 】

図 7 A は、散乱光の C C D 画像 7 0 0 の一例を示し、図 7 B は、C C D 画像 7 0 0 を使って決定された散乱光の強度の垂直方向に平均化されたプロット 7 1 0 を示す。図示されている実施例では、図 7 A 内の垂直軸線は C C D 上の垂直ピクセル位置に対応し、水平軸線は C C D 上の水平方向のピクセル位置に対応する。より明るいピクセルは、より強い強度の散乱光を示し、より暗いピクセルは比較的弱い強度の散乱光を示す。図 7 B 内の垂直軸線は、水平方向のピクセル位置に対応する水平軸方向の特定ピクセル幅（バンド）の光強度に対応する。この強度は、図 7 B において任意の単位で測定したものである。垂直方向の平均は、一部のピクセルレベルのノイズを除去するように働く。図 7 B に示されたこの分布は、散乱導波管の構造および実験パラメータ、例えばレーザービームとの整合によって決定される。

【 0 0 4 0 】

M A T L A B 7.1 を使用して書き込んだカスタムコードを使用して散乱光の捕捉画像、例えば図 7 A ~ B に示された画像を処理することによって暗号化鍵を発生した。暗号化鍵の発生を実証するために、散乱光の未処理の C C D 画像をビットマップとして M A T L A B に導入した。後述するように画像をフィルタにかけ、ほぼガウス分布する乱数のスト

10

20

30

40

50

リングを抽出し、暗号化鍵を形成し、これを2進数に変換する。簡単なテキストラインのユーザーインターフェースを使用して、暗号化すべきメッセージを入力し、このメッセージも2進数に変換する。実証化のために、暗号化鍵による簡単なビットごとにXOR演算を実行することによってメッセージを暗号化した。同じ演算パラメータのもとで発生させた同一の暗号化鍵を使って、メッセージの暗号を解読した。

【0041】

図8Aおよび8Bは、直線方向の位置および回転角方向の位置のそれぞれの関数としての相互相関係数を示す。双方の図の垂直軸線は、相関化の値を任意の単位で示し、図8Aの水平軸線はミリメートルを単位とする直線方向の位置を示し、図8Bの水平軸線は、ミリラジアンを単位とする回転角方向の位置を示す。入射レーザービームに対する散乱導波管の直線方向の位置および回転角方向の向きを操作することにより、整合に対する導波管の感度、潜在的な暗号化鍵スペースのサイズの定量化および再整合並びに繰り返し測定に対する散乱光パターンの一貫性の特徴を定めることが可能となった。整合による散乱光の感度をテストするために、導波管を5μmの増分量だけ直線方向にシフトし、0.05°（～0.87ミリラジアン）の増分量だけ、入射端面を中心として回転した。強度分布の相互相関性は、それぞれ約25μmおよび5ミリラジアンでゼロ相関性を示した。従って、単一入射波長に対し、1cm×1cmの単一の散乱導波管により、約10⁻⁶の相関性のないパターンを発生できる。

【0042】

わずかな機械的不整合に対する散乱光パターンの感受性および乱れのような環境的要因は、これらノイズソースを除去するための望ましいある種のフィルタリングを行うことができる。図示された実施例では、この目的のために一次元のガウスウェーブレットマルチスケールフィルタを使用する。このフィルタの核は次のとおりである。

【数1】

$$g(n,x)=C_n*\exp[-x^2/2\sigma_n^2+i2\pi f_n x]$$

ここで、 g = 信号によってたたみ込むべきフィルタ核であり、
 n は屈折率であり、
 x = 空間座標であり、
 C = 正規化定数であり、
 σ = ガウス包絡線の標準偏差であり、
 f = フィルタの中心周波数である。

【0043】

1オクターブの周波数ステップでステップングする繰り返しフィルタとしてフィルタを使用し、周波数領域において一定の1オクターブのバンド幅を提供するように標準偏差を選択する。かかる状態で、ピクセルレベルのノイズおよび小さい不整合に起因するばらつきを除き、システムパラメータの所定の組による所定の乱数を繰り返し発生できるようにする。本明細書の開示に利害を有する当業者であれば、本発明は一次元のガウスウェーブレットマルチスケールフィルタだけに限定されないことが理解できるはずである。別の実施例では、望ましいフィルタまたはフィルタリング技術を使用できる。

【0044】

本発明は、当業者に明らかな、異なるが同等な態様で発明を変形し、実施できるので、これまで開示した特定の実施例は単に説明のためのものに過ぎない。更に、特許請求の範囲に記載したもの以外に、図示した構造の細部について限定を意図するものではない。従って、これまで説明した特定の実施例は変形または変更が可能であり、かかる変形のいずれも、本発明の要旨の範囲内と見なされることは明らかである。従って、本明細書におい

て求める保護範囲は特許請求の範囲に記載されている。

【図面の簡単な説明】

【0045】

【図1】本発明に係わる乱数暗号化鍵のような乱数を発生するためのシステムを概念的に示す。

【図2A】本発明に係わる散乱導波管の第1実施例の側面図を概念的に示す。

【図2B】本発明に係わる散乱導波管の第1実施例の上から見た平面図を概念的に示す。

【図3】本発明に係わる散乱導波管の第2実施例を概念的に示す。

【図4】本発明に係わる画像捕捉および処理システムの一実施例を概念的に示す。

【図5】本発明に従い、散乱光に基づき、乱数を形成する方法の一実施例を概念的に示す

10

【図6A】本発明に従い、単結晶シリコン基板上に構成された対称的なポリマー製のスラブ導波管の一実施例を概念的に示す。

【図6B】本発明に従い、単結晶シリコン基板上に構成された対称的なポリマー製のスラブ導波管の一実施例を概念的に示す。

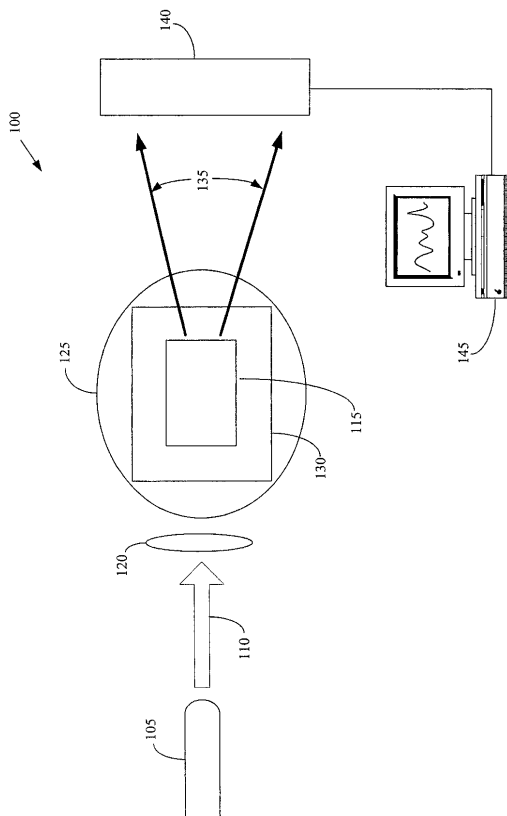
【図7A】散乱光のCCD画像の一例を示す。

【図7B】散乱光の強度の垂直方向に平均したプロットを示す。

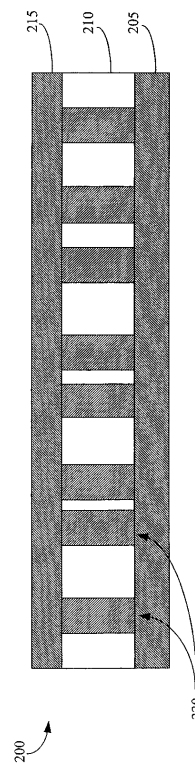
【図8A】直線上の位置の関数としての相互相関性の係数を示す。

【図8B】回転角方向の位置の関数としての相互相関性の係数を示す。

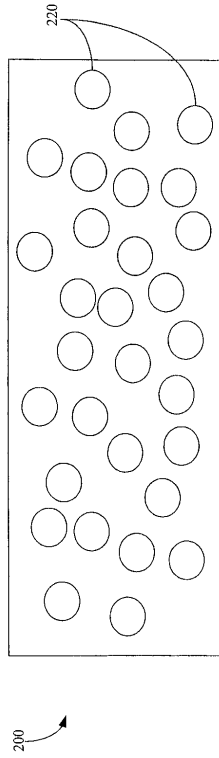
【図1】



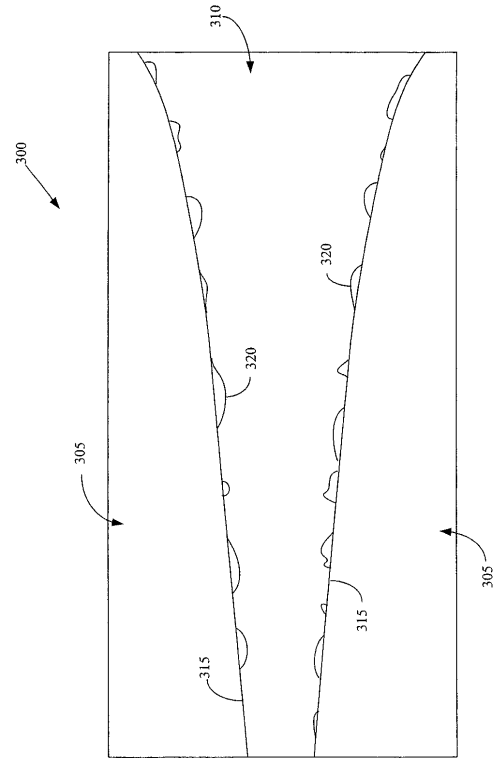
【図2A】



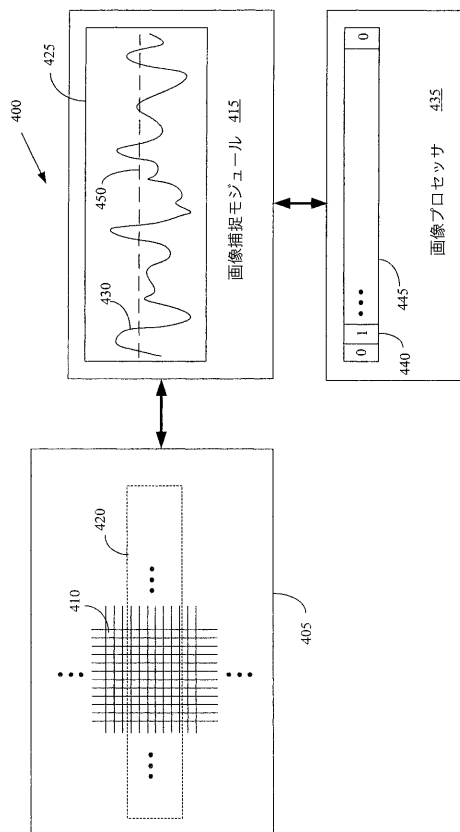
【図 2 B】



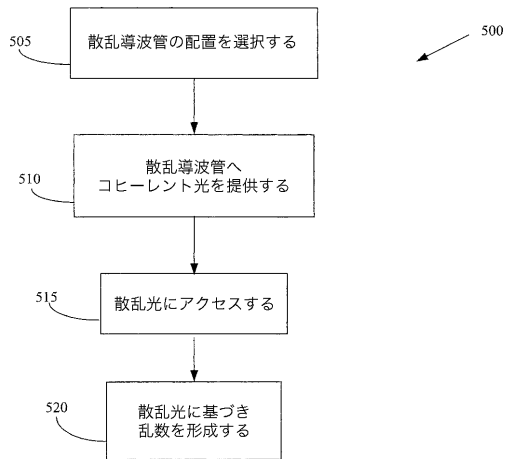
【図 3】



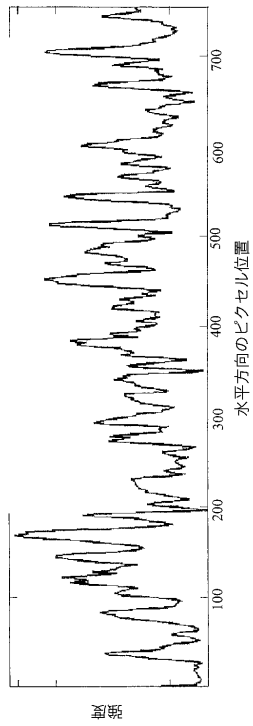
【図 4】



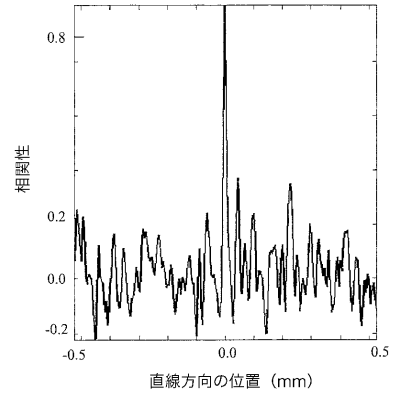
【図 5】



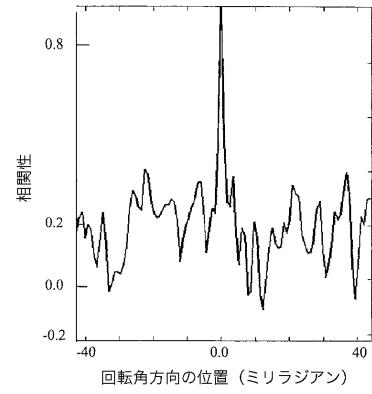
【図 7 B】



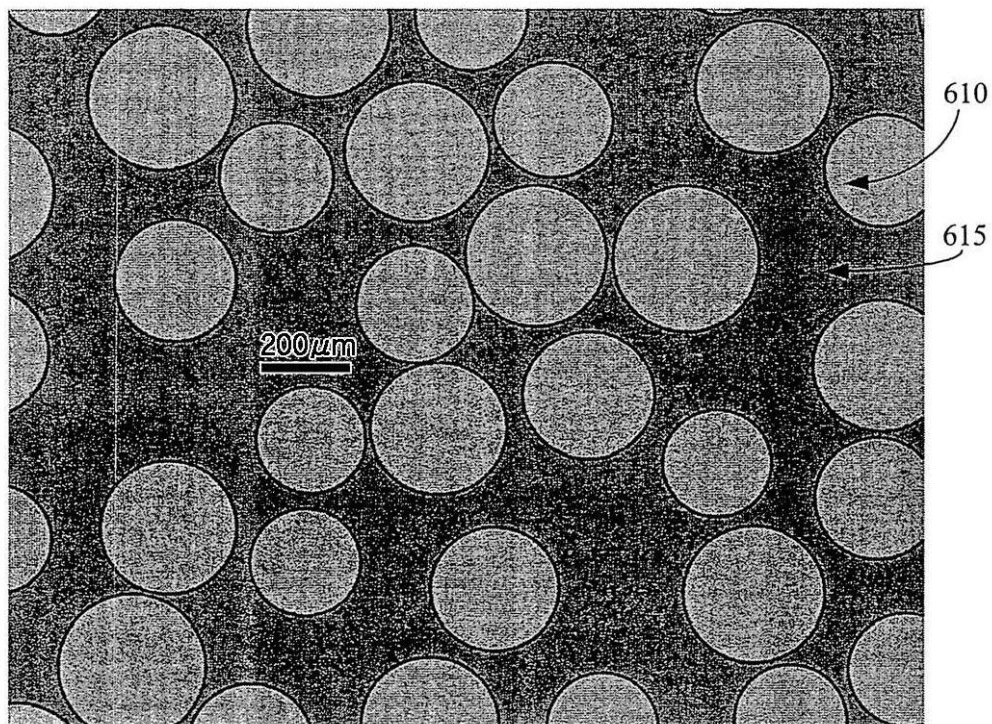
【図 8 A】



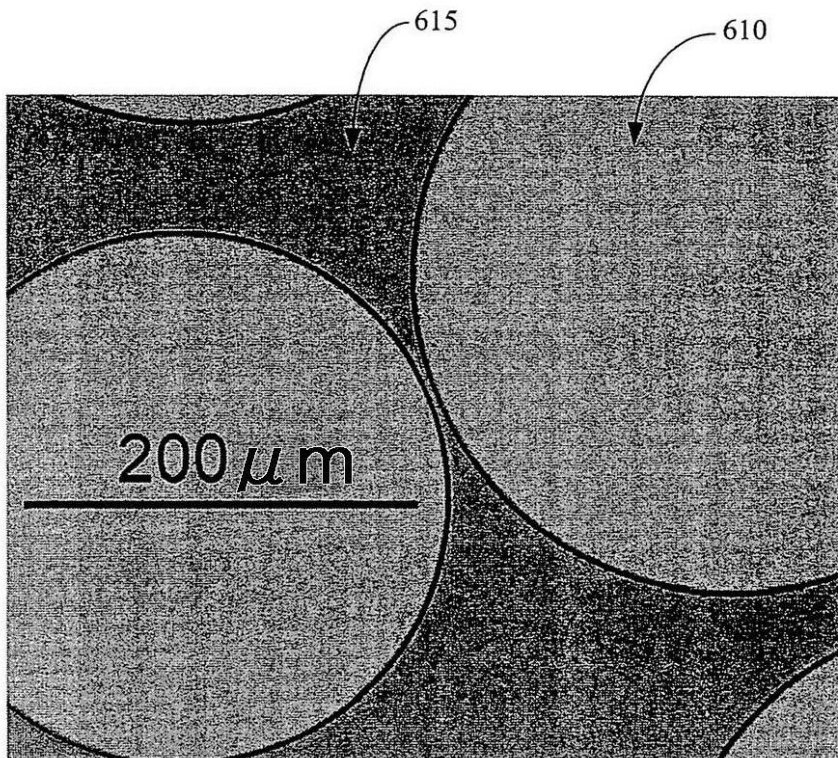
【図 8 B】



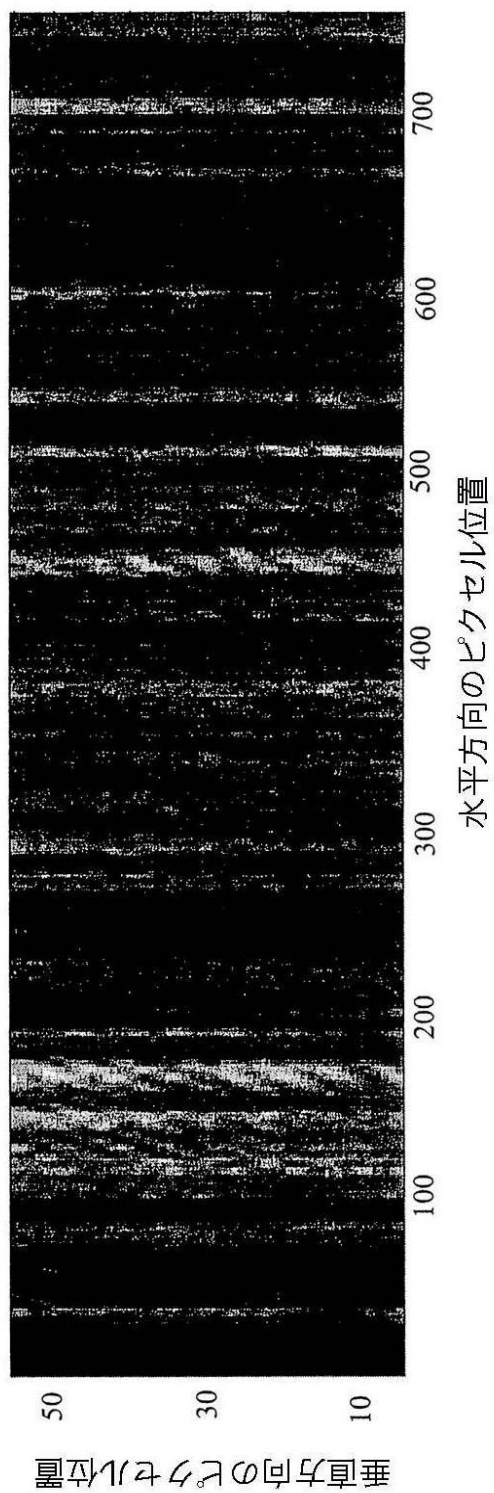
【図 6 A】



【図 6 B】



【図 7 A】



フロントページの続き

- (72)発明者 クラップ、テリー、ブイ .
イギリス国、ハートフォードシャー、ビショップス ストートフォード、 ロバート ウォレス
クローズ、 8
- (72)発明者 デシェイザー、デーヴィッド、ジェイ .
アメリカ合衆国、ミシガン、ベイ シティ、 シックス ストリート 1304

審査官 田中 友章

- (56)参考文献 特表2005-526299(JP,A)
特開2000-276329(JP,A)

(58)調査した分野(Int.Cl. , DB名)

G06F 7/58
G09C 1/00