

(19)日本国特許庁(JP)

(12)特許公報(B1)

(11)特許番号
特許第7672180号
(P7672180)

(45)発行日 令和7年5月7日(2025.5.7)

(24)登録日 令和7年4月24日(2025.4.24)

(51)国際特許分類

F I

G 0 6 F 7/58 (2006.01) G 0 6 F 7/58 6 8 0

請求項の数 10 (全21頁)

(21)出願番号	特願2024-106532(P2024-106532)	(73)特許権者	511055522
(22)出願日	令和6年7月2日(2024.7.2)		ケーエヌユーーインダストリー コーポ
審査請求日	令和6年7月2日(2024.7.2)		レーション ファウンデーション
(31)優先権主張番号	10-2024-0030450		KNU-INDUSTRY COOPE
(32)優先日	令和6年3月4日(2024.3.4)		RATION FOUNDATION
(33)優先権主張国・地域又は機関			大韓民国 2 4 3 4 1 カンウォンド,
	韓国(KR)		チュンチョン-シ, カンウォンデハク-
(31)優先権主張番号	10-2024-0050017		ギル 1
(32)優先日	令和6年4月15日(2024.4.15)		1, Gangwondaehak-g i
(33)優先権主張国・地域又は機関			l, Chuncheon-s i, Gan
	韓国(KR)		gwon-do 2 4 3 4 1, Repu
			blic of Korea
		(74)代理人	110004381
			弁理士法人I T O H
		(72)発明者	ジョン, ヒジェ
			最終頁に続く

(54)【発明の名称】 血液サンプルを基に乱数を生成するシステム及びそれを利用した方法

(57)【特許請求の範囲】

【請求項1】

血液サンプルを基に乱数を生成するシステムであって、
予め設定された血液サンプルを供給するサンプルローディングモジュールと、
前記サンプルローディングモジュールによって提供された血液サンプルに光を照射する
光照射モジュールであって、予め指定された関心領域（ROI）に移動させた血液サンプ
ルを対象に光を照射する光照射モジュールと、
前記光照射モジュールを利用し、前記関心領域に位置する血液サンプルの画像を予め設
定された方式でキャプチャすることで、原本スペckル画像を獲得する画像生成モジュ
ールと、
前記画像生成モジュールから生成された前記原本スペckル画像を予め設定された方式
で処理して乱数を生成する乱数生成モジュールと
を含み、前記乱数生成モジュールは、前記原本スペckル画像を構成するピクセル値を
対象に0または1のビットに分類する二進化過程を行い、二進化画像を生成する二進化画
像生成部を含み、
前記乱数生成モジュールは、前記二進化画像生成部によって獲得された二進化画像を対
象に、フォン・ノイマン後処理方式を適用することで第1処理画像を生成するフォン・ノ
イマン抽出部を更に含む、システム。

【請求項2】

前記フォン・ノイマン抽出部は、

前記第1処理画像を対象に、2 P - T O - V N (T w o - P a s s T u p l e - O u t p u t v o n N e u m a n n) 方式を更に適用することで第2処理画像を生成する
請求項1に記載のシステム。

【請求項3】

前記フォン・ノイマン抽出部は、

1 P - T O - V N (O n e - P a s s T u p l e - O u t p u t v o n N e u m a n n) 方式を適用し、

2つのビットを一つのセットにして予め設定された方式で処理し、前記予め設定された方式は一つのセットが同じビットの重複であれば前記セットを除去する方式である、

請求項2に記載のシステム。

10

【請求項4】

前記フォン・ノイマン抽出部は、

一つのセットが同じビットの重複であって、前記セットが除去された残りのビットを基準に、互いに異なるビットでセットが構成される場合、前記セットを構成する第1及び第2ビットのうち第1または第2ビットのみを維持する、

請求項3に記載のシステム。

【請求項5】

前記フォン・ノイマン抽出部は、

前記1 P - T O - V N方式によって、除去されたセットをクアッド (Q u a d) に更にグルーピングし、前記クアッドは第1セット及び第2セットで構成され、前記第1及び第2セットの異同に基づいて前記第1及び第2セットを除去するか又は維持するかを決定する、

請求項4に記載のシステム。

20

【請求項6】

前記フォン・ノイマン抽出部は、

前記第1及び第2セットが互いに異なる場合、前記第1及び第2セットを更に復元させる、

請求項5に記載のシステム。

【請求項7】

前記乱数生成モジュールは、

前記二進化画像生成部によって生成された二進化画像を対象に、画像スクランブリングを行って前処理画像を生成する画像スクランブリング部を更に含み、

前記フォン・ノイマン抽出部は、

前記画像スクランブリング部によって生成された前記前処理画像を対象に第1及び第2処理画像が生成される、

請求項2に記載のシステム。

30

【請求項8】

血液サンプルを基に乱数を生成する方法であって、

(a 1) サンプルローディングモジュールによって予め設定された血液サンプルを供給するステップと、

(a 2) 光照射モジュールによって前記サンプルローディングモジュールによって提供された血液サンプルに光を照射するステップであって、予め指定された関心領域に移動させた血液サンプルを対象に光を照射するステップと、

(a 3) 前記光照射モジュールを利用し、前記関心領域に位置する血液サンプルの画像を予め設定された方式でキャプチャすることで、原本スペckル画像を獲得するステップと、

(a 4) 前記ステップ (a 3) で生成された前記原本スペckル画像を予め設定された方式で処理して乱数を生成するステップと

を含み、前記ステップ (a 4) は、

(a 4 1) 前記原本スペckル画像を構成するピクセル値を対象に0または1のビット

40

50

に分類する二進化過程を行い、二進化画像を生成するステップと、

(a 4 2) 前記ステップ (a 4 1) で獲得された二進化画像を対象に、フォン・ノイマン後処理方式を適用することで第 1 処理画像を生成するステップを含む、方法。

【請求項 9】

前記ステップ (a 4) は、

(a 4 3) 前記ステップ (a 4 2) で生成された前記第 1 処理画像を対象に、2 P - T O - V N 方式を更に適用することで第 2 処理画像を生成するステップを更に含む、

請求項 8 に記載の方法。

【請求項 10】

前記ステップ (a 4 2) の前に、

(a 4 2 - 0) 前記ステップ (a 4 1) で生成された二進化画像を対象に、画像スクランプリングを行って前処理画像を生成するステップを更に含む、

請求項 9 に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は血液サンプルを基に乱数を生成するシステム及びそれを利用した方法に関し、より詳しくは、2 P - T O - V N (Two - Pass Tuple - Output von Neumann) 方式が適用された乱数生成システムに関する技術である。

【背景技術】

【0002】

この部分に記述された内容は単に本実施例に関する背景情報を提供するだけであって、従来技術を構成するものではない。

【0003】

インターネットをはじめとする有無線通信の使用の急速に拡大されるにつれ、通信ネットワークのセキュリティ問題は国家、企業、金融上の重要機密の保護及び個人のプライバシーの保護の側面でその重要性が次第に増大しつつある。P S A など数学的な計算複雑性に基づく暗号システムは量子コンピュータが開発されれば根本的に解読が可能であると判断されるため、その対策が求められている。

【0004】

計算複雑性に基づく暗号システムに比べ、ワンタイムパッド (One Time Pad : O T P) を利用した暗号方式は最も安全な暗号方式と知られている。ワンタイムパッドを利用してストリーム暗号 (Stream Cipher) を生成すれば、迅速で安全に暗号化された通信を行い得る。このようなワンタイムパッドを生成するために、乱数生成器 (Random Number Generator、RNG) が使用される。

【0005】

乱数生成器システムの進化と持続的な開発は、暗号化分野の未来のための重要な礎となっている。このような RNG システムは予測が難しいだけでなく、殆ど不可能なキーを生成する役割のため全ての暗号化システムの中核となっている。

【0006】

このような予測不可能性は、今日のデジタル世界で必要な機能である高いレベルのセキュリティを保障し得る。乱数生成器には主にアルゴリズムと物理的という 2 つのタイプがある。擬似乱数生成器 (Pseudo Random Number Generators、PRNG) と知られているアルゴリズム生成器は、複雑な数学公式を使用して一連の数字を生成する。

【0007】

PRNG は便利で効率的であるが、生成された乱数はランダム性テストを通過しても逆設計及び予測が可能であるという短所がある。それに対し、物理的 (または実際) 乱数生成器は確率論的物理的プロセスからランダム性を導出し得る。このようなプロセスは完全な情報で理論的に予測可能であるが、時間及び計算リソースの制限のため実質的には予測

10

20

30

40

50

できない。

【0008】

RNGはこのような特性のため、キーの生成、デジタル署名の生成、暗号化のための初期化ベクトル、セキュリティ保存のためのソルト値の生成をはじめとする多様なサイバーセキュリティ作業で主な役割をし、IoTドメインを超えて相互連結されたシステムのサイバーセキュリティ要求事項を解決し得る。

【0009】

新しく浮かび上がっている関心分野のうち一つは、セキュリティ強化のために光学的物理的な複製防止機能を使用することである。Di Falcoなどの研究。シリコンチップによって促進される乱れているシステムは完璧な秘密性を備えた暗号化システムを達成するために活用され得ることを示している。

10

【0010】

しかし、物理基盤のRNGには固有な課題があるということに留意することが重要である。例えば、ラバランプから任意のパターンをキャプチャすることは革新的な方法であるが、帯域幅が制限されている。発光ダイオードと携帯電話のカメラを使用する他の方法は、光の量子変動からランダム性をキャプチャするが、設定が非常に複雑である。よって、RNGシステムの環境は最近数年間変化を経ており、人為的に生成された従来のRNGには固有のセキュリティ脆弱点が含まれていることが明らかになっている。

【0011】

このような脆弱点のため、更に予測不可能で本質的にランダムなバイオメトリクスRNGシステムへの転換が触発された。変化は生物学的システムが不可能ではないとしても、人為的に複製することは難しいレベルの複雑性とランダム性を含む場合が多いという事実を認める。

20

【0012】

よって、最近のRNG技術ではスペックル(Speckle)パターンを利用したRNGの生成に重点を置こうと試みている。このような技術の主な目標は経済性と携帯性の均衡を達成することである。2つともこのようなシステムの広範囲な採択と適用のための必須要素と評価されている。

【0013】

スペックルパターン生成領域において、RNG及び光子の物理的複製解除機能の発展は一貫性のある光の下でスペックルパターンが生成されるように、紙の自然な質感のような材料の本質的なランダム性に依存する場合が多い。例えば、光導波管は検証済みのランダム性によってMbit/sの速度で乱数を生成する能力を示す。

30

【0014】

また、エアロゲルのスペックルパターンを基に全光学物理的複製解除機能(Fractalocchietal.)を開発し、安全なキーの生成を達成している。しかし、このような技術にはレーザービームを体積散乱媒体に通過させて静的スペックルパターンをキャプチャする作業が含まれる。この接近方法は革新的であるが、コストの効率性と高速乱数生成に対する新しい課題が提起され得る。加えて、このようなRNGが提供する向上されたセキュリティ機能にもかかわらず、産業現場での適用は制限的である。主な障害物はサンプルの製作及び獲得速度に関する高いコストにある。このようなコストが増加すれば一般に購買速度が向上される。

40

【0015】

逆に、コストが下がれば速度が遅くなる場合が多く、最適化が複雑になるという衝突関係が現れるが、この問題のため優れた性能を提供すると共に製造コストを大きく節減するRNGシステムが必要となっている。

【0016】

RNG分野の従来技術としては、特許文献1(フォン・ノイマン後処理時の乱数出力信号の連続性を確保するための方法及び装置)が開示される。前記従来技術は乱数出力信号の非連続性を解決する内容を開示するが、メモリバッファに乱数を保存し、保存された乱

50

数が全て消費されれば、他の構成によって予備乱数を出力することで、システムの速度を向上させると共に、コストを下げるという経済性をその効果とする。

【0017】

但し、前記従来技術はフォン・ノイマン後処理を利用した乱数出力技術のみを開示するだけであって、血流または血液サンプルの適用及び結合可能性については全く開示していない。

【先行技術文献】

【特許文献】

【0018】

【文献】韓国登録特許第10-1925787号公報

10

【発明の概要】

【発明が解決しようとする課題】

【0019】

本発明は上述した問題点を解決するために案出されたものであって、高速乱数生成が可能でありながらもコストの効率性を極大化し、また、生成された乱数のランダム性を向上させることで、生成された乱数の信頼性を担保するシステムを提供することにその目的がある。

【0020】

但し、本発明が解決しようとする技術的課題は上述した課題に限らず、言及されていない他の課題は以下に記載の発明の説明から当業者に明確に理解されるはずである。

20

【課題を解決するための手段】

【0021】

本発明の一側面によるシステムは、血液サンプルを基に乱数を生成するシステムであって、予め設定された血液サンプルを供給するサンプルローディングモジュールと、前記サンプルローディングモジュールによって提供された血液サンプルに光を照射し、この場合に、予め指定された関心領域 (region of interest、ROI) に移動させた血液サンプルを対象に光を照射する光照射モジュールと、前記光照射モジュールを利用し、前記関心領域に位置する血液サンプルの画像を予め設定された方式でキャプチャすることで、原本スペックル画像を獲得する画像生成モジュールと、前記画像生成モジュールから生成された前記原本スペックル画像を予め設定された方式で処理して乱数を生成する乱数生成モジュールと、を含む。

30

【0022】

好ましくは、前記乱数生成モジュールは、前記原本スペックル画像を構成するピクセル値を対象に0または1のビット (bit) に分類する二進化過程を行い、二進化 (binary) 画像を生成する二進化画像生成部を含み得る。

【0023】

好ましくは、前記乱数生成モジュールは、前記二進化画像生成部によって獲得された二進化画像を対象に、フォン・ノイマン (von Neumann) 後処理方式を適用することで第1処理画像を生成するフォン・ノイマン抽出部を更に含み得る。

【0024】

好ましくは、前記フォン・ノイマン抽出部は、前記第1処理画像を対象に、2P-T O-VN方式を更に適用することで第2処理画像を生成し得る。

40

【0025】

好ましくは、前記フォン・ノイマン抽出部は、1P-T O-VN (One-Pass Tuple-Output von Neumann) 方式を適用し、2つのビットを一つのセットにして予め設定された方式で処理するが、前記予め設定された方式は一つのセットが同じビットの重複であれば前記セットを除去する方式であり得る。

【0026】

好ましくは、前記フォン・ノイマン抽出部は、一つのセットが同じビットの重複であって、前記セットが除去された状態で、残りのビットを基準に、互いに異なるビットでセッ

50

トが構成される場合、前記セットを構成する第1及び第2ビットのうち第1または第2ビットのみを維持する方式であり得る。

【0027】

好ましくは、前記フォン・ノイマン抽出部は、前記1P-T-O-V-N方式によって、除去されたセットをクアッド(Quad)に更にグルーピングするが、前記クアッドは第1セット及び第2セットで構成され、前記第1及び第2セットの同一可否に基づいて前記第1及び第2セットの除去維持可否を決定し得る。

【0028】

好ましくは、前記フォン・ノイマン抽出部は、前記第1及び第2セットが互いに異なる場合、前記第1及び第2セットを更に復元させ得る。

【0029】

好ましくは、前記乱数生成モジュールは、前記二進化画像生成部によって生成された二進化画像を対象に、画像スクランブリング(image scrambling)を行って前処理画像を生成する画像スクランブリング部を更に含み、前記フォン・ノイマン抽出部は、前記画像スクランブリング部によって生成された前記前処理画像を対象に第1及び第2処理画像が生成され得る。

【0030】

また、本発明は血液サンプルを基に乱数を生成する方法であって、(a1)サンプルローディングモジュールによって予め設定された血液サンプルを供給するステップと、(a2)光照射モジュールによって前記サンプルローディングモジュールによって提供された血液サンプルに光を照射し、この場合に、予め指定された関心領域に移動された血液サンプルを対象に光を照射するステップと、(a3)前記光照射モジュールを利用し、前記関心領域に位置する血液サンプルの画像を予め設定された方式でキャプチャすることで、原本スペックル画像を獲得するステップと、(a4)前記ステップ(a3)で生成された前記原本スペックル画像を予め設定された方式で処理して乱数を生成するステップと、を含む方法を提供する。

【0031】

好ましくは、前記ステップ(a4)は、(a41)前記原本スペックル画像を構成するピクセル値を対象に0または1のビットに分類する二進化過程を行い、二進化画像を生成するステップと、(a42)前記ステップ(a41)で獲得された二進化画像を対象に、フォン・ノイマン後処理方式を適用することで第1処理画像を生成するステップと、(a43)前記ステップ(a42)で生成された前記第1処理画像を対象に、2P-T-O-V-N方式を更に適用することで第2処理画像を生成するステップと、を含み得る。

【0032】

好ましくは、前記ステップ(a42)の前に、(a42-0)前記ステップ(a41)で生成された二進化画像を対象に、画像スクランブリングを行って前処理画像を生成するステップを更に含み得る。

【発明の効果】

【0033】

本発明の一実施例によると、血流を活用してスペックルパターンを生成する革新的なシステムを提示する。

【0034】

特に、多様な細胞構成要素が豊富な血液固有の特性は生成されたスペックルの複雑性とエントロピーを向上させることで、生成された乱数のランダム性を増大させ得る。

【0035】

本発明はシステムの迅速な速度でスペックルパターンをキャプチャし得、極めて少量の血液のみを必要とするため、これは乱数生成に関するコストと獲得時間をいずれも最小化してシステム接近性を向上させ得る。

【0036】

また、本発明の一実施例によるシステムは、生成されたランダムビットが偏向しないよ

10

20

30

40

50

うに設計された2P-T-O-VN方式を適用することで、生成されたビット数を増やすと共にシステムの全般的な予測不可能性と強力なセキュリティ性を提供し得る。

【0037】

その他にも本発明の様々な実施例によって、様々な異なる追加的な効果が達成され得る。このような本発明の様々な効果については各実施例で詳細に説明するか、当業者が容易に理解し得る効果についてはその説明を省略する。

【図面の簡単な説明】

【0038】

本発明に添付される以下の図面は本発明の好ましい実施例を例示するものであり、後述する発明の詳細な説明と共に本発明の技術思想を更に理解させる役割をするものがあるため、本発明はそのような図面に記載の事項に限って解釈されてはならない。

【図1】本発明の一実施例によるシステムの全体構成を示すブロック図である。

【図2】本発明の一実施例によるシステムの血液サンプル検査装置を示す模式図である。

【図3】図2の血液サンプル検査装置におけるサンプルローディングモジュールを例示的に示す模式図である。

【図4】本発明の一実施例によるシステムを利用して乱数を生成する過程を概略的に示す概要図である。

【図5】本発明の一実施例によるシステムのフォン・ノイマン抽出部における処理過程を概略的に示すブロック図である。

【図6】図5の過程を説明するための一例示である。

【図7】本発明の一実施例による方法の順序図である。

【図8】図7のステップS40を細部的に区分した順序図である。

【図9】原本スペckル画像(OSI)、第1処理画像(CVN方式)、第2処理画像(2P-T-O-VN方式)それぞれのスペckル逆相関時間を比較したグラフである。

【図10】原本スペckル画像(OSI)、第1処理画像(CVN方式)、第2処理画像(2P-T-O-VN方式)の乱数行列特性を比較したグラフである。

【図11】第1処理画像(CVN方式)及び第2処理画像(2P-T-O-VN方式)のスペckルビット生成率とそれぞれの画像を示す結果である。

【図12a】原本スペckル画像(OSI)、第1処理画像(CVN方式)、第2処理画像(2P-T-O-VN方式)を示す一例示的画像である。

【図12b】画像スクランプリングが適用された一例示的画像である。

【図13】本発明の一実施例によるシステムを利用して生成された乱数に対するNIST統計的ランダム性テストの結果を示す表である。

【発明を実施するための形態】

【0039】

以下、添付した図面を参照して本発明の好ましい実施例を詳細に説明する。その前に、本明細書及び特許請求の範囲で使用された用語や単語は通常的であるか辞書的な意味に限って解釈されてはならず、発明者は自らの発明を最善の方法で説明するために用語の概念を適切に定義し得るとの原則に立脚して本発明の技術的思想に符合する意味と概念で解釈されるべきである。

【0040】

本発明は多様な変更を加えることができ、多様な実施例を有することができるゆえ、特定実施例を図面に例示し、発明を実施するための形態に詳細に説明する。しかし、これは本発明を特定な実施形態に対して限定しようとするのではなく、本発明の思想及び技術範囲に含まれる全ての変更、均等物乃至代替物を含むと理解すべきである。各図面を説明しながら、類似した参照符号を類似した構成要素に対して使用している。

【0041】

第1、第2、A、Bなどの用語は多様な構成要素を説明するのに使用されるが、構成要素は用語によって限定されてはならない。用語は一つの構造要素を他の構成要素から区別する目的にのみ使用される。例えば、本発明の権利範囲を逸脱しないながらも第1構成要

10

20

30

40

50

素は第2構成要素と命名されてもよく、類似して第2構成要素も第1構成要素と命名され得る。「及び／または」という用語は、複数の関連する記載された項目の組み合わせまたは複数の関連する記載された項目のうちいずれかの項目を含む。

【0042】

ある構成要素が他の構成要素に「連結されて」いるか「接続されて」いると言及されれば、その他の構成要素に直接連結されているかまたは接続されていてもよいが、中間に他の構成要素が存在し得ると理解すべきである。反面、ある構成要素が他の構成要素に「直接連結」されているか「直接接続」されていると言及されれば、その中間に他の構成要素が存在しないと理解すべきである。

【0043】

本出願で使用された用語は単に特定の実施例を説明するために使用されたものであって、本発明を限定しようとする意図ではない。単数の表面は文脈上明白に異なるように意味しない限り、複数の表現を含む。本出願において、「含む」または「有する」などの用語は明細書の上に記載された特徴、数字、ステップ、動作、構成要素、部品またはこれらを組み合わせたものが存在することを指定するものであって、一つまたはそれ以上の他の特徴や数字、ステップ、動作、構成要素、部品またはこれらを組み合わせたものの存在または付加可能性を予め排除しないと理解すべきである。

【0044】

異なるように定義されない限り、ここで使用される技術的か科学的な用語を含む全ての用語は、本発明が属する技術分野における通常の知識を有する者によって一般的に理解されるものと同じ意味を有する。一般的に使用される辞書に定義されているものと同じ用語は、関連技術の文脈上有する意味と一致する意味を有すると解析すべきであり、本出願で明白に定義しない限り、理想的にまたは過度に形式的な意味で解析されない。

【0045】

図1は、本発明の一実施例によるシステムの全体構成を示すブロック図である。図1を参照して、本発明の一実施例によるシステムを説明する。

【0046】

システム10は、サンプルローディングモジュール400と、光照射モジュール100と、画像生成モジュール200と、乱数生成モジュール300とを含む。ここで、乱数生成モジュール300は本システムに含まれているプロセッサ内に保存されているプログラムとして実行され得る。

【0047】

図2は本発明の一実施例によるシステムの血液サンプル検査装置を示す模式図であり、図3は図2の血液サンプル検査装置におけるサンプルローディングモジュールを例示的に示す模式図である。

【0048】

図2及び図3を共に参照して説明する。

【0049】

光照射モジュール100は、血液サンプルSに光を照射するように構成され得る。一例として、血液サンプルS内の血液には、図3に示したように例示的に赤血球R、血小板Pなどが含まれ得る。また、前記光は一定範囲の波長（例えば、532nm）を有するレーザーであってもよいが、これに限らない。

【0050】

血液サンプルSはネズミから抽出されて蒸留された脱イオン水（*deionized water*）内に含まれ得るが、これに限らない。本出願人はプロトコルGIST-2019-015を厳しく遵守しており、公式的に承認された全ての方法は実験報告のためのARRIVE指針を遵守していることを明示する。

【0051】

詳しくは、本出願人は尾静脈切開術によって体重250～280gの間の12～13週の雄Sprague Dawleyネズミから血液サンプルを収集した。そのために動物

10

20

30

40

50

をイソフルランで麻酔させている間に23Gの針を介して血液1mlを投与した。11匹のネズミグループに対してこのような血液収集を行っており、後続実験のためにサンプルをクエン酸チューブ（カタログ#363083、9NC 0.109M Buffered Trisodium Citrate、BD Vacutainer、USA）に直ちに保管した。

【0052】

画像生成モジュール200は、光が照射された血液サンプルSのスペックル画像（Speckle Image）を獲得するように構成され得る。詳しくは、画像生成モジュール200は、撮影部210と、第1レンズ220と、開口230と、第2レンズ240と、偏光板250と、反射鏡260と、コリメータ270と、カプラ280とを含み得る。

10

【0053】

撮影部210は、光が照射された血液サンプルSのスペックル画像を撮影して獲得するように構成され得る。一例として、撮影部210はCMOSカメラ（Neo 5.5 sCMOS、Andor Technology Ltd.、Belfast、UK）であってもよいが、これに限らない。このCMOSカメラは0.8ミリ秒の露出時間と秒当たり1250フレームの高いフレーム速度で作動し、後続データを生成するために128×512ピクセルの解像度でスペックル画像を円滑にキャプチャする。

【0054】

血液サンプルSのスペックル画像は、光が血液サンプルSから反射されるか光が血液サンプルSを透過する際に発生する干渉によって不規則に生成されるスペックルパターン（Speckle Pattern）を含み得る。一例として、1000個のフレームで総7つの実験データセットを構成し、実験データを前処理するためにこれをそれぞれ32×256ピクセルで構成された8つの仕切りで分けて、総56個のセットを利用した。

20

【0055】

第1レンズ200は対物レンズであって、撮影部210と血液サンプルSが配置されるサンプルローディングモジュール400の間に配置され得る。開口230は絞りであって、撮影部210と第1レンズ220との間に配置され得る。第2レンズ240はチューブレンズであって、撮影部210と開口230との間に配置され得る。

【0056】

前記偏光板250は第2レンズ240と開口230との間に配置され得る。

30

【0057】

この際、開口230、第2レンズ240、及び偏光板250は、撮影部210によって獲得される血液サンプルSのスペックル画像におけるコントラスト（contrast）を向上させるために備えられ得る。

【0058】

反射鏡260は、光照射モジュール100から照射された光を反射して血液サンプルSに入射させるように構成され得る。この際、反射鏡260は少なくとも一つ以上備えられ得る。

【0059】

コリメータ（collimator）270は、血液サンプルSが配置されるサンプルローディングモジュール400と反射鏡260との間に配置され得る。

40

【0060】

カプラ280は光カプラ（optical coupler）であって、コリメータ270と反射鏡260との間に配置され得る。

【0061】

サンプルローディングモジュール400は血液サンプルSを移動させるように構成され得る。一例として、サンプルローディングモジュール400はPDMS（Polydimethylsiloxane）材質を含み得る。サンプルローディングモジュール400は、本体410と、注入部420と、移動チャンネル230と、排出部440とを含み得る。

【0062】

50

本体 410 はサンプルローディングモジュール 400 の全体的な形状を構成し得る。注入部 420 は血液サンプル S が本体 410 の内部に流入される部分であり得る。

【0063】

移動チャネル 430 は本体 410 に備えられ、前記注入部 420 を介して流入された血液サンプル S を移動させる構成であり得る。ここで、移動チャネル 430 は「マイクロチャネル」と称され得る。光照射モジュール 100 によって照射される光（例えば、 $\lambda = 532 \text{ nm}$ のレーザ光）が移動チャネル 430 を通過した後、ROI 領域は第 1 レンズ 220 によってキャプチャされ得る。それによって「原本スペックル画像」が獲得されるが、前記原本スペックル画像は後述する乱数生成モジュール 300 によってランダムビットを生成するように構成される。

10

【0064】

移動チャネル 430 はマイクロチャネルを構成するために、ソフトフォトリソグラフィを適用して長さ 45 mm、高さ 45 μm 、幅 1 mm の正確な寸法でチャネルが設計され得る。一例として、本出願人は様々な標準プロセスに従って PDMS スラブを製造しており、PDMS Sylgard 184 A/B (Dow Corning Korea Ltd.) で構成されるこのスラブは酸素プラズマ処理によってカバーガラスに接着されている。

【0065】

移動チャネル 430 はポンプ、ソレノイドバルブ、3 方向バルブ、及び死容積を説明する 50 ml 注射器が統合された真空発生器で構成される。ポンプは流れを調節するソレノイドバルブを使用し、変動回収モードで 200 μL の一定な体積で試料採集を制御し得る。

20

【0066】

排出部 440 は、移動チャネル 430 内で流動する血液サンプル S を本体 410 の外部に排出する部分であり得る。ポンピングモジュール 500 は、ポンプ 510 と、移動管 520 と、第 1 バルブ 530 と、第 2 バルブ 540 と、死容積チェンバ 550 とを含み得る。

【0067】

ポンピングモジュール 500 は、前記サンプルローディングモジュール 400 に連結されて真空圧によって血液サンプル S をサンプルローディングモジュール 400 の方に移動させる構成であり得る。

【0068】

ポンプ 510 は真空ポンプであって、真空圧を形成して血液サンプル S をサンプルローディングモジュール 400 の本体 410 の方に移動させ得る。一例として、ポンプ 510 はシリンジポンプ (syringe pump) であり得る。移動管 520 は、ポンプ 510 によって形成された真空圧によって血液サンプル S が本体 410 の方に移動される管であり得る。

30

【0069】

第 1 バルブ 530 は、移動管 520 に備えられて本体 410 に加えられる真空圧を調節するように構成され得る。一例として、第 1 バルブ 530 はソレノイドバルブであり得る。第 2 バルブ 540 及び死容積チェンバ 550 は移動管 520 に備えられて血液サンプル S の移動を緩衝し得る。この際、死容積チェンバ 550 は第 2 バルブ 540 を介して移動管 520 に結合され得る。一例として、第 2 バルブ 540 は三方バルブ (3-way valve) であり得、死容積チェンバ 550 は空き空間で形成される容器であり得る。

40

【0070】

乱数生成モジュール 300 は、画像生成モジュール 200 から生成された原本スペックル画像を処理して乱数を生成するように構成される。一例として、乱数生成モジュール 300 演算処理機能を有する CPU、GPU、AP、またはその組み合わせの形態などで具現され得、必要によって DRAM、フラッシュメモリ、SSD、その他の多様な形態のメモリと共に備えられ得る。

【0071】

乱数生成モジュール 300 は、二進化画像生成部 310 と、フォン・ノイマン抽出部 3

50

20と、画像スクランブリング部330とを含み得る。

【0072】

図4は本発明の一実施例によるシステムを利用して乱数を生成する過程を概略的に示す概要図であり、図5は本発明の一実施例によるシステムのフォン・ノイマン抽出部における処理過程を概略的に示すブロック図である。

【0073】

二進化画像生成部310は、原本スペckル画像を構成するピクセル値を対象に0または1のビットに分類する二進化過程を行い、二進化画像を生成するように構成される。つまり、原本スペckル画像を二進化画像に変換させる。

【0074】

画像スクランブリング部330は二進化画像にスクランブリングを行うように構成される。SCI (Scrambling Code Injection) とは画像にスクランブリングコードを注入することを意味する。フォン・ノイマン抽出部320を経る前に画像をスクランブリングすることで、ビット生成速度を向上させ得る。

【0075】

後述する第1及び第1処理画像はいずれも画像スクランブリング部330によってスクランブリングが行われた状態で生成される画像であり得る。

【0076】

フォン・ノイマン抽出部320は、二進化画像生成部310によって獲得された二進化画像を対象にフォン・ノイマン後処理方式を適用することで、第1処理画像を生成する。次に、第1処理画像を対象に2P-T-O-VN方式を更に適用することで第2処理画像を生成し得る。

【0077】

ここで、フォン・ノイマン後処理方式は2P-T-O-VN方式とは対比する方式であって、1P-T-O-VN方式と理解され得る。つまり、2P-T-O-VN方式は1P-T-O-VN方式に追加にパスを経る過程を含む。

【0078】

図6は図5での過程を説明するための一例であって、本発明の方式は図6に示された方式に制限されない。

【0079】

フォン・ノイマン抽出部320は1P-T-O-VN方式を先に経てから、更に別途のパスを経ることで、2P-T-O-VN方式で処理され得る。

【0080】

図6を参照すると、2つのビットを一つのセットにして区分する過程を経る。ここで、一つのセットが同じビットの重複であればセットを除去し得る。一例として、「00」または「11」のセットは削除されてもよい。

【0081】

次に、一つのセットが同じビットの重複であって、前記セットが除去された状態で、残りのビットを基準に、互いに異なるビットでセットが構成される場合、前記セットを構成する第1及び第2ビットのうち第1または第2ビットのみを維持する方式に設定され得、このように1P-T-O-VN方式が完了される。一例として、「01」または「10」であれば、「01」の「0」または「10」の「1」のような最初のビットのみ維持し得る。

【0082】

次に、フォン・ノイマン抽出部320は追加のパスを行うように構成される。それによってビットの偏向性を下げ得る。

【0083】

2P-T-O-VN方式は、1P-T-O-VN方式によって除去されたセットをクアッドに更にグルーピングするが、クアッドは第1セット及び第2セットで構成され、第1及び第2セットの同一可否に基づいて第1及び第2セットの除去維持可否を決定する過程を更に経ると理解され得る。ここで、第1及び第2セットが互いに異なる場合、前記第1及び

10

20

30

40

50

第2セットを更に復元させ得る。一例として、「0011」または「1100」などのように前後が異なる捨てられたセットは更に保存するように設定され得る。

【0084】

1P-T-O-VN方式と知られているフォン・ノイマン(CVN)偏向性除去方法が厳しい圧縮のためビット数を大きく減らすに対し、2P-T-O-VN方式はビット維持と偏向性除去の間の適切な均衡を提供し得る。2P-T-O-VN方式は初期に廃棄されたビットを再評価することで、図6で見られるように実際のアプリケーションに更に適合したデータボリュームを生成するため、強力で使用可能な暗号化キー(乱数)を生成するため前記CVNの卓越した代案になり得る。

【0085】

図7は本発明の一実施例による方法の順序図であり、図8は図7のステップS40を細部的に区分した順序図である。

【0086】

図7及び図8を参照して方法について説明するが、上述した内容と重複する説明は省略する。

【0087】

本発明の一実施例による方法は、ステップS10乃至ステップS40を含む。

【0088】

ステップS10は、サンプルローディングモジュール400によって予め設定された血液サンプルを供給するステップである。

【0089】

ステップS20は、光照射モジュール100によってサンプルローディングモジュール400によって提供された血液サンプルに光を照射し、この場合に、予め指定された関心領域に移動された血液サンプルを対象に光を照射するステップである。

【0090】

ステップS30は、光照射モジュール100を利用し、前記関心領域に位置する血液サンプルの画像を予め設定された方式でキャプチャすることで原本スペックル画像を獲得するステップである。

【0091】

ステップS40は、ステップS30で生成された原本スペックル画像を予め設定された方式で処理して乱数を生成するステップである。

【0092】

ここで、ステップS40は更にステップS41乃至ステップS43を含み得る。

【0093】

ステップS41は、原本スペックル画像を構成するピクセル値を対象に0または1のビットに分類する二進化過程を行い、二進化画像を生成するステップである。

【0094】

ステップS411は、ステップS41で生成された二進化画像を対象に、画像スクランブリングを行って前処理画像を生成するステップである。

【0095】

ステップS42は、ステップS41で獲得した二進化画像を対象にフォン・ノイマン後処理方式を適用することで、第1処理画像を生成するステップである。

【0096】

ステップS43は、ステップS42で生成された第1処理画像を対象に2P-T-O-VN方式を更に適用することで、第2処理画像を生成するステップである。

【0097】

図9は、原本スペックル画像(OSI)、第1処理画像(CVN方式)、第2処理画像(2P-T-O-VN方式)それぞれのスペックル逆相関時間を比較したグラフである。本発明は血流を基に乱数を生成する方式の結果に対する検証を行っている。

【0098】

10

20

30

40

50

図9を参照して説明すると、逆相関時間は推定されたランダム性の主な尺度である。実際及びスクランプリングされたランダムビットに比べ、56個の原本スペックル画像に対する自己相関曲線を示す。原本スペックル画像を派生されたランダムビットと比べる際、逆相関時間は大きな差を示す。原本スペックル画像の平均逆相関時間は ± 0.43 の標準偏差で3.05秒であり、CVN (Classic von Neumann) 画像の後処理された一連のランダムビット、スクランプリングが含まれたCVN、2P-T-O-VN方式、及びスクランプリング画像がある2P-T-O-VN方式は、それぞれ 1.542 ± 0.019 、 1.538 ± 0.018 、 1.551 ± 0.017 、及び 1.529 ± 0.013 の著しく一貫した平均及び標準偏差を示す。このように密接してクラスタリングされた値は56個の多様な画像の間で相関関係が低いか存在しないことを示し、ランダム性

10

【0099】

図10は、原本スペックル画像(OSI)、第1処理画像(CVN方式)、第2処理画像(2P-T-O-VN方式)の乱数行列特性を比較したグラフである。

【0100】

図10を参照して、ビットの均一性と相関関係の差の比較を説明する。データの潜在的な偏向を解決するために、歪みを反映して平均0.626の原本スペックル画像のビットの均一性を検査した。2P-T-O-VN方式を適用した後、2P-T-O-VN方式のみで処理されたケースと、スクランプリングコードの挿入と結合された2つのデータセット両方に対して0.500の例示的なビットの均一性を確認した。0.500とは「1」と「0」ビットの理想的な均衡を示すと理解され得る。

20

【0101】

(b)乃至(d)に示したように、56個の原本画像と処理されたスペックル画像に対する相関分析を使用して追加に調べた結果、処理されたデータセットは原本画像より約2,270倍のずっと低い相関値達成したと示されている。

【0102】

また、処理された2つのデータセットを比較する際、SCI処理が含まれた2P-T-O-VN方式は、2P-T-O-VN方式のみ適用された画像に比べ相関関係値が18.34%減少したと示されており、これ位はSCI処理が相関関係を更に悪化させると理解され得る。

30

【0103】

(c)と(d)において、対角線領域の外部の相関値が0に近づけば相関関係が減少したことを示す。

【0104】

原本スペックル画像に対する特定の相関関係のメトリックは、標準偏差は0.016264で、平均は0.01896と確認され、処理されたデータは0.000453と0.000343の相関値を有する2P-T-O-VN画像とSCIがある2P-T-O-VN画像が0.000383と0.000296のずっと低い相関関係を生成するなど、著しい改善を示す。このような結果はビットの均一性を達成し、相関関係を最小化する2P-T-O-VN方式の効率性を強力に強調し得、血流スペックルを基盤にする乱数生成の統計的信頼性を検証し得る。

40

【0105】

図11は、第1処理画像(CVN方式)及び第2処理画像(2P-T-O-VN方式)のスペックルビット生成率とそれぞれの画像を示す結果である。

【0106】

図11を参照すると、(a)は原本スペックルビットから生成されたビット生成率のグラフである。スペックルビットは810万ビットで構成される。各画像の平均及び標準偏差は、それぞれ 16.65 ± 2.27 、 23.37 ± 0.49 、 52.35 ± 3.34 、及び 67.70 ± 2.44 と演算される。

【0107】

50

これらはNISTランダム性テストによって予測不可能性についてテストを済ましている。NISTランダム性テストは、ランダムビットのランダム性の品質を決定するために、本出願人は国立標準技術研究所（National Institute of Standards and Technology Statistical Test Suite、NIST）を使用して一連の統計テストを行った。

【0108】

ちなみに、NISTテストはバイナリーシーケンスのランダム性を定量的に評価するように設計され、NISTテストスイートは15個の個別テストで構成されるが、各テストは二進シーケンスのランダム性の多様な側面を定量的に測定するように設計される。

【0109】

テストには頻度、ブロック頻度、実行、LRO（最長実行）、連続、近似エントロピー、累積合計（Cumsums）の評価が含まれ、本出願人が行った評価には56個の互いに異なるランダムビットから二進シーケンスを集計して7つの統計テストに対する適切なストリーム長さを保障する作業が含まれている。

【0110】

ここで、 $P(s)$ はサンプルの経路長さの分布であり、 s は経路長さであり、 τ は遅延時間、 l^* は伝送平均自由経路、 τ_o は媒体の特性崩壊時間を意味する。

【0111】

自己相関は0乃至1の値になり、時間遅延が増加することで該当値は0に近く落ちるべきであるが、これはそれ以上最初の画像と比べ相関関係がないことを意味する。バイオミメティクスから影響を受けた真のランダムビットの生成を確認するために、血液が移動チャネル430を通過しながら、50%地点で斑点パターン画像の時系列で連続した2つの画像間の相関関係を測定した。

【0112】

【数1】

$$g_1(\tau) = \int_0^\infty P(s) \exp \left[\left(-\frac{2\tau}{\tau_o} \right) \frac{s}{l^*} \right]$$

また、データ分析（ビットの均一性、平均相関関係）。ランダムビットの性能を評価するためにデジタル化されたキーを検査する。ここで、ビットの均一性はランダムビット内で「0」と「1」ビットの分布（割合）がいかに均衡をなしているのかを評価する。

【0113】

【数2】

$$\text{Bit uniformity} = \frac{1}{s} \sum_{l=1}^s K_l$$

ランダムビットシーケンスの均一性は、時々長さ「s」の二進文字列で「1」のビット数であるハミング重みを決定して評価される。特定のビットセットの場合、「0」と「1」ビットの均等な分布を反映してハミング重みが0.5近くになれば所望の均一性が達成される。

【0114】

また、相関行列を利用して画像間の相関関係を調べる。比較の客観性を保障するために、本発明の方式によって得られたランダムビットを定量化し一致させて、均一なビットの行列を作って調べている（例えば、原本スペckル画像：7.8Mビット、CVN画像：1.02Mビット、SCIがあるCVN：1.8Mビット、2P-T-O-VN画像：3.3Mビット、SCIがある2P-T-O-VN：4.8Mビット）。

【 0 1 1 5 】

【 数 3 】

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}}$$

ここで、相関関係を定量化するためにピアソン相関係数の公式を使用し得る。数式において、 $\bar{x}$ 及び $\bar{y}$ は x 及び y 値の平均を示し、 r で表されるピアソン相関係数は 0 に近いほど 2 つのセットのランダムビットの間に有意な相関関係がないことを示す。

10

【 0 1 1 6 】

図 1 3 は本発明の一実施例によるシステムを利用して生成された乱数に対する N I S T 統計的ランダム性テストの結果を示す表であり、本出願人はこれをいずれもパスしたことを確認し得る。

【 0 1 1 7 】

図 1 2 a は原本スペckル画像 (O S I)、第 1 処理画像 (C V N 方式)、第 2 処理画像 (2 P - T O - V N 方式) を示す一例示的画像であり、図 1 2 b は画像スクランブリングが適用された一例示的画像である。

【 0 1 1 8 】

20

図 1 2 を参照すると、スペckルパターンは 0 と 1 ビットで構成される予測不可能なランダムビットを生成しており、高出力及び性能向上のために画像スクランブリング及び 2 P - T O - V N 方式を使用して追加のランダム性を統合した。

【 0 1 1 9 】

(b) を参照すると、S C I が含まれた画像の総ピクセルはそれぞれ 4 9 9 8 0 (6 0 X 8 3 3) ピクセル ((a) を参考) と 5 6 5 2 0 (6 0 X 9 4 2) ピクセル ((b) を参考) であるため、スクランブリングに影響を受けることを確認し得る。

【 0 1 2 0 】

以上のように、本発明はたとえ限定された実施例によって説明されたが、本発明はこれによって限定されず、本発明の属する技術分野における通常の知識を有する者によって本発明の技術思想と以下に記載される特許請求の範囲の均等範囲内で多様な修正及び変形が可能なことはもちろんである。

30

【 符号の説明 】

【 0 1 2 1 】

1 0 : システム

1 0 0 : 光照射モジュール

2 0 0 : 画像生成モジュール

3 0 0 : 乱数生成モジュール

4 0 0 : サンプルローディングモジュール

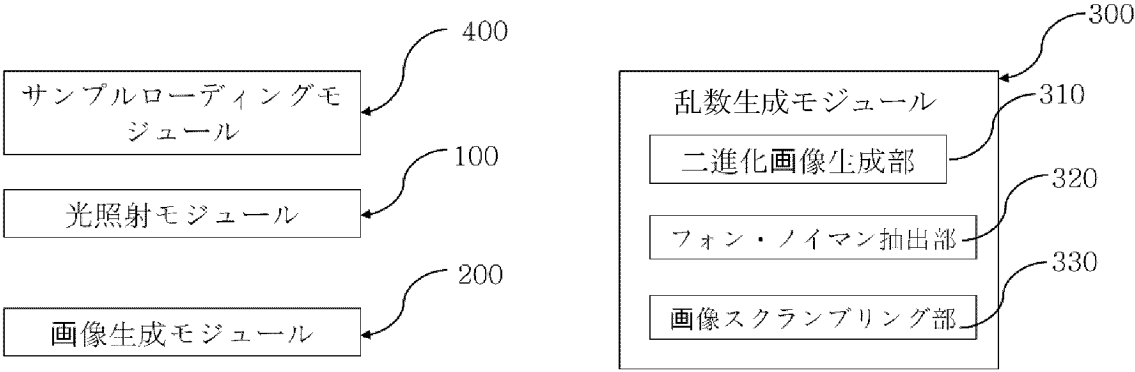
40

【要約】 (修正有)

【課題】 高速乱数生成が可能でありながらもコストの効率性を極大化し、かつ、血液サンプルを基に生成された乱数のランダム性を向上させることで、生成された乱数の信頼性を担保するシステム及び方法を提供する。

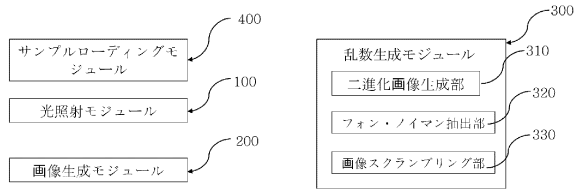
【解決手段】 血液サンプルを基に乱数を生成するシステムは、予め設定された血液サンプルを供給するサンプルローディングモジュールとサンプルローディングモジュールによって提供され、予め指定された関心領域 (region of interest、ROI) に移動させた血液サンプルを対象に光を照射する光照射モジュールと、光照射モジュールを利用し、関心領域に位置する血液サンプルの画像を予め設定された方式でキャプチャすることで、原本スペックル (speckle) 画像を獲得する画像生成モジュールと、画像生成モジュールから生成された原本スペックル画像を予め設定された方式で処理して乱数を生成する乱数生成モジュールと、を含む。

【選択図】 図 1

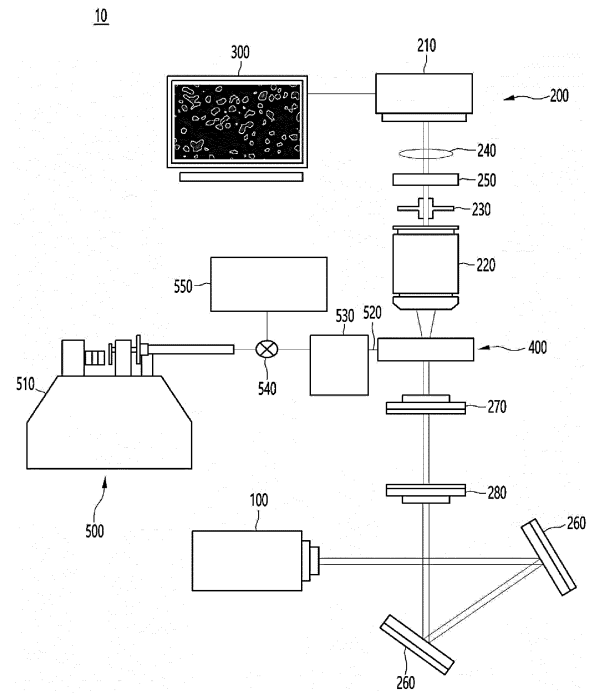


【凶面】

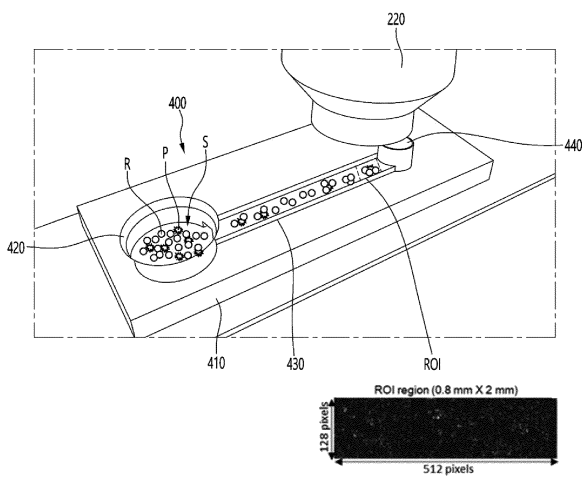
【図 1】



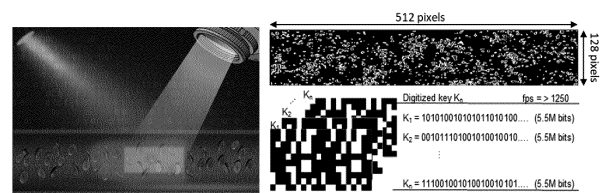
【図 2】



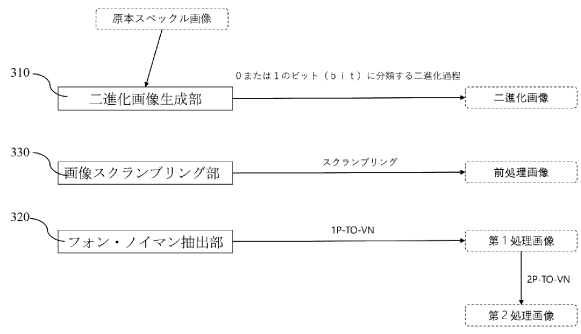
【圖 3】



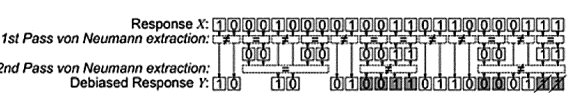
【図 4】



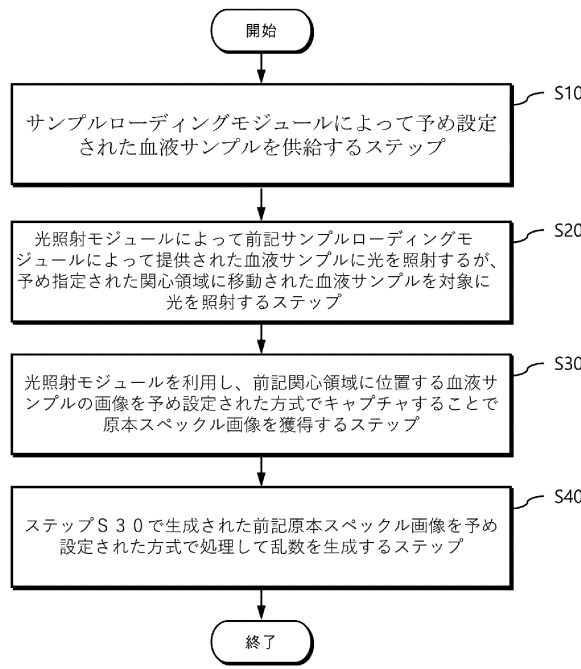
【図 5】



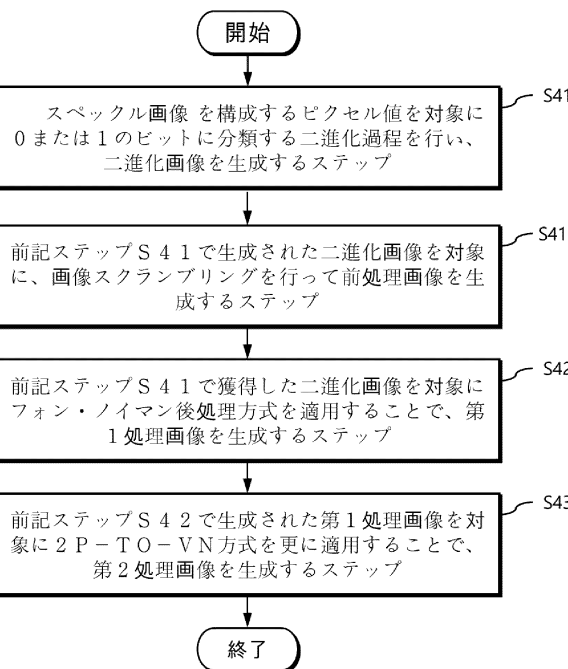
【図 6】



【図 7】



【図 8】



10

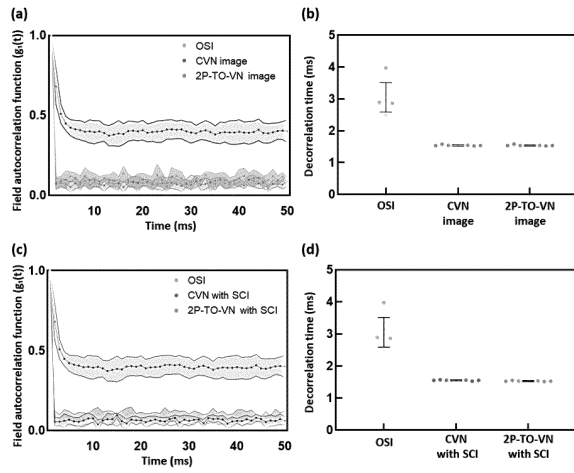
20

30

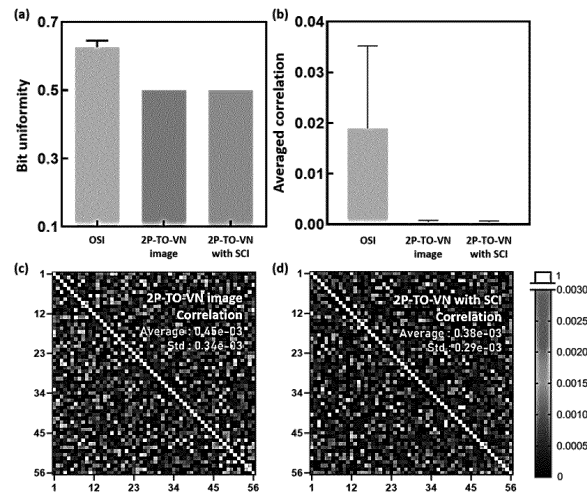
40

50

【図 9】

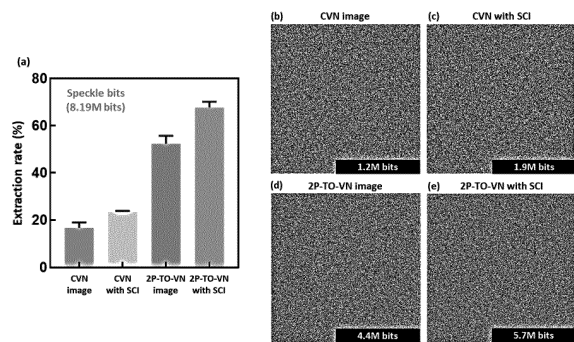


【図 10】

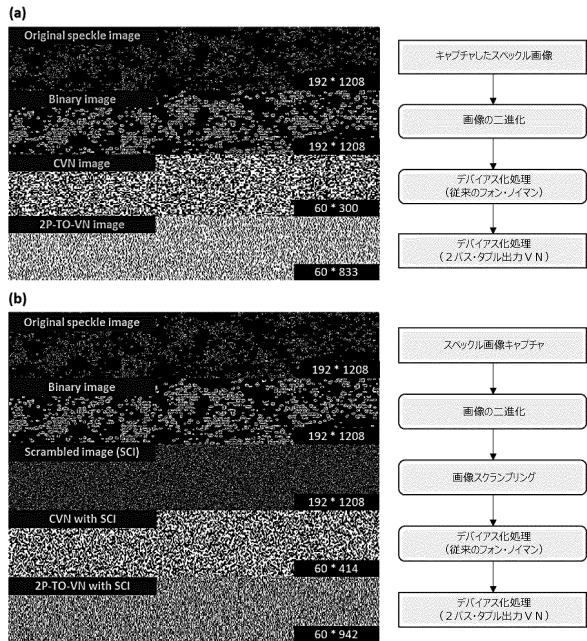


10

【図 11】



【図 12】



20

30

40

50

【図 13】

(a)

NIST statistical test ⁽¹⁾	p-value	Proportion	Result ⁽²⁾
Frequency	0.000000	60/60	Pass
BlockFrequency	0.049821	60/60	Pass
CumulativeSums	0.000000	60/60	Pass
	0.000000	60/60	Pass
Runs	0.498475	59/60	Pass
LongestRun	0.505842	59/60	Pass
ApproximateEntropy	0.341105	58/60	Pass
Serial	0.466500	59/60	Pass
	0.449781	59/60	Pass

(b)

NIST statistical test ⁽¹⁾	p-value	Proportion	Result ⁽²⁾
Frequency	0.000000	60/60	Pass
BlockFrequency	0.000000	60/60	Pass
CumulativeSums	0.000000	60/60	Pass
	0.000000	60/60	Pass
Runs	0.463253	60/60	Pass
LongestRun	0.462783	59/60	Pass
ApproximateEntropy	0.442474	59/60	Pass
Serial	0.439529	59/60	Pass
	0.497110	59/60	Pass

(1) NIST統計テストは56個の異なるランダム・ビットから得られた4,088ビットのシーケンスを使用することを含む。
次いで、このビット・シーケンスは60個のシーケンスに分割され、各シーケンスは8000ビットから成る。χ²分布を用いてp値分布の決定係数 (goodness-of-fit) が予測された分布と比較される。結果のp値が0.0001以上である場合に限り、ビット・シーケンスはランダムであるとみなされる。

(2) パスレートが、60回のテストのうち56より大きな最低レートを越える場合に、テストは合格したと考えられる。

10

20

30

40

50

フロントページの続き

大韓民国 6 2 2 4 6 クァンジュ クァンサンーグ ワンボドウルー口 1 3 2 ボンーギル 3 5 6
0 7 - 2 1 0 4

(72)発明者 ユン, インクォン

大韓民国 2 4 3 4 2 カンウォンード チュンチョンーシ ペクリョンー口 2 3 ボンーギル 2 7
3 0 1

審査官 佐賀野 秀一

(56)参考文献 特開 2 0 1 0 - 2 7 1 8 8 8 (J P , A)

特開 2 0 2 4 - 0 1 3 3 3 5 (J P , A)

特表 2 0 0 9 - 5 1 6 4 4 5 (J P , A)

(58)調査した分野 (Int.Cl., DB名)

G 0 6 F 7 / 5 8