(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2013-242584
(P2013-242584A)
(43)公開日　平成25年12月5日(2013.12.5)

(51)Int.Cl.			F I			テーマコード（参考）
G09C	1/00	(2006.01)	G09C	1/00	650B	5C075
H04N	1/44	(2006.01)	H04N	1/44		5J104

審査請求 有　請求項の数 10　ＯＬ　（全 13 頁）

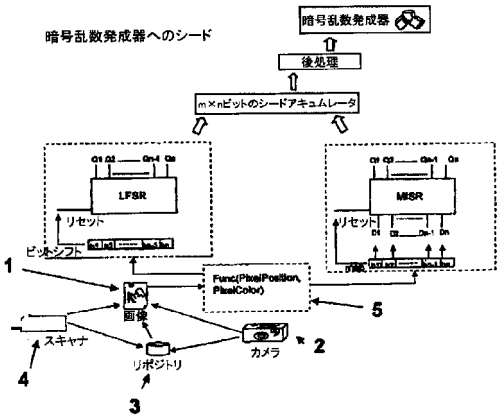
(21)出願番号　特願2013-145551 (P2013-145551)
(22)出願日　平成25年7月11日 (2013.7.11)
(62)分割の表示　特願2008-554647 (P2008-554647)の分割
原出願日　平成19年2月12日 (2007.2.12)
(31)優先権主張番号　06003029.3
(32)優先日　平成18年2月15日 (2006.2.15)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　508246618
ジェイクリプト　リミテッド
イギリス　アールエム１１　２キュービー　ホーンチャーチ　ネルムズ　クレッセント　３０
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100086771
弁理士　西島　孝喜
(74)代理人　100109070
弁理士　須田　洋之
(74)代理人　100122563
弁理士　越柴　絵里

最終頁に続く

(54)【発明の名称】暗号乱数発生器にシードを与えるための方法及び装置

(57)【要約】
【課題】本発明は、暗号乱数発生器にシードを与えるための方法及び装置を提供することを目的とする。
【解決手段】暗号乱数発生器にシードを与えるために画像を使用する。入力した画像の画素が選択されて、その各々に関連する位置情報及び色情報が与えられる。選択された画素に関連するこの位置情報と色情報とを用いて所定数のビットを計算し、次にこれらのビットを使用して暗号乱数発生器にシードを与える。ユーザは、カメラ、スキャナ、又はリポジトリで画像を入力することができる。
【選択図】図４



【特許請求の範囲】
【請求項１】
暗号乱数発生器にシード(seed)を与えるための方法であって、
画像（１）の少なくとも一部を入力するステップと、
前記画像（１）の画素を選択し、該画素の各々に関連する位置情報及び色情報が与えられるステップと、
前記選択された画素に関連する前記位置情報と前記色情報とを用いて所定数のビットを計算するステップと、
前記暗号乱数発生器にシードを与えるために、前記計算された数のビットを出力するステップと、
を含むことを特徴とする方法。
【請求項２】
暗号乱数を発生させるための方法であって、
画像（１）の少なくとも一部を入力するステップと、
前記画像（１）の画素を選択し、該画素の各々に関連する位置情報及び色情報が与えられるステップと、
前記選択された画素に関連する前記位置情報と前記色情報とを用いて所定数のビットを計算するステップと、
前記計算された数のビットを暗号乱数として出力するステップと、
を含むことを特徴とする方法。
【請求項３】
前記画像（１）の少なくとも一部を入力する前記ステップは、前記画像（１）を選択したユーザにより実行される、
ことを特徴とする請求項１又は２に記載の方法。
【請求項４】
前記入力ステップは、後のステップで使用される複数の画像（１）を入力するステップを含む、
ことを特徴とする請求項１～３の何れか１項に記載の方法。
【請求項５】
前記入力ステップは、カメラ（２）、及び／又はスキャナ（４）、及び／又はリポジトリ（３）を使用して行われ、少なくとも１つの画像（１）が前記リポジトリ（３）に格納される、
ことを特徴とする請求項１～４の何れか１項に記載の方法。
【請求項６】
前記入力ステップは、
前記入力された画像のサイズ、色濃度、及び／又は色変化に基づいてこの画像の適合性を反映する良度指数を計算するステップと、
前記計算された良度指数を所定のしきい値と比較するステップと、
前記比較の結果、前記画像（１）が適切でなければ、拒否するか、或いは警告を出すステップと、
前記比較の結果、前記画像（１）が適切であれば、前記画像（１）を受け入れるステップと、
をさらに含むことを特徴とする請求項１～５の何れか１項に記載の方法。
【請求項７】
既に使用された画像を拒否するか、及び／又は警告を出すことにより、画像の再選択を防止する、
ことを特徴とする請求項６に記載の方法。
【請求項８】
前記画像（１）の画素を選択する前記ステップは、
前記画像（１）の画素の一部をランダムに選択し、特に、現在選択されている画素の前

記色及び／又は位置に基づいて前記次の画素を選択するステップを含む、
ことを特徴とする請求項１～７の何れか１項に記載の方法。
【請求項９】
前記所定数のビットを計算する前記ステップは、線形フィードバックシフトレジスタ又は多入力シフトレジスタを使用する、
ことを特徴とする請求項１～８の何れか１項に記載の方法。
【請求項１０】
前記画像（１）の画素を選択する前記ステップは、画素サイズをレジスタ素子数と整合するステップをさらに含む、
ことを特徴とする請求項１～９の何れか１項に記載の方法。
【請求項１１】
前記所定数のビットを計算する前記ステップは、ビットをバッファすることにより前記所定数の出力ビットを変更できるようにするステップを含む、
ことを特徴とする請求項１～１０の何れか１項に記載の方法。
【請求項１２】
請求項１～請求項１１の何れか１項に記載の方法により得られる乱数シード(seed)。
【請求項１３】
暗号乱数発生器にシード(seed)を与えるための装置であって、
画像（１）の少なくとも一部を入力するようにされた入力手段と、
前記画像（１）の画素を選択し、該画素の各々に関連する位置情報及び色情報が与えられるようにされた選択手段（５）と、
前記選択された画素に関連する前記位置情報と前記色情報とを用いて所定数のビットを計算するようにされた計算手段と、
前記暗号乱数発生器にシードを与えるために、前記計算された数のビットを出力するようにされた出力手段と、
を備えることを特徴とする装置。
【請求項１４】
暗号乱数を発生させるための装置であって、
画像（１）の少なくとも一部を入力するようにされた入力手段と、
前記画像（１）の画素を選択し、該画素の各々に関連する位置情報及び色情報が与えられるようにされた選択手段（５）と、
前記選択された画素に関連する前記位置情報と前記色情報とを用いて所定数のビットを計算するようにされた計算手段と、
前記計算された数のビットを暗号乱数として出力するようにされた出力手段と、
を備えることを特徴とする装置。
【請求項１５】
前記入力手段は、ユーザが前記画像（１）を選択できるようにされた、
ことを特徴とする請求項１３又は１４に記載の装置。
【請求項１６】
前記入力手段は、後のステップで使用される複数の画像（１）を入力できるようにされた、
ことを特徴とする請求項１３～１５の何れか１項に記載の装置。
【請求項１７】
前記入力手段は、カメラ（２）、及び／又はスキャナ（４）、及び／又はリポジトリ（３）であり、少なくとも１つの画像（１）が前記リポジトリ（３）に格納される、
ことを特徴とする請求項１３～１６の何れか１項に記載の装置。
【請求項１８】
前記入力手段は、
前記入力された画像のサイズ、色濃度、及び／又は色変化に基づいてこの画像の適合性を反映する良度指数を計算するようにされた計算手段と、

前記計算された良度指数を所定のしきい値と比較するようにされた比較手段と、
前記比較の結果、前記画像（１）が適切でなければ、拒否するか、或いは警告を出すようにされた信号送信手段と、
をさらに含み、前記装置は、
前記比較の結果、前記画像（１）が適切であれば、前記画像（１）を受け入れるようにされた、
ことを特徴とする請求項１３～１７の何れか１項に記載の装置。
【請求項１９】
前記比較手段及び信号送信手段はさらに、後の時点における画像の再選択を防ぐようになっている、
ことを特徴とする請求項１８に記載の装置。
【請求項２０】
前記選択手段（５）は、
前記画像（１）の画素の一部をランダムに選択し、特に、現在選択されている画素の前記色及び／又は位置に基づいて前記次の画素を選択するようにされたランダム選択手段を含む、
ことを特徴とする請求項１３～１９の何れか１項に記載の装置。
【請求項２１】
前記計算手段は、線形フィードバックシフトレジスタ又は多入力シフトレジスタを含む、
ことを特徴とする請求項１３～２０の何れか１項に記載の装置。
【請求項２２】
前記選択手段はさらに、画素サイズをレジスタ素子数と整合するようにされた、
ことを特徴とする請求項１３～２１の何れか１項に記載の装置。
【請求項２３】
前記計算手段は、ビットをバッファすることにより前記所定数の出力ビットを変更できるようにされた格納手段を含む、
ことを特徴とする請求項１３～２２の何れか１項に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に暗号の分野に関し、より具体的には、暗号乱数発生器にシード(seed)を与えるための方法及び装置に関する。
【背景技術】
【０００２】
乱数発生器（ＲＮＧ）は、宝くじ、ギャンブル機器、科学モデル及び金融モデルのシミュレーション、プログラム及びアルゴリズムのテスト、方程式の解法、及びコンピュータセキュリティなどの様々な電子的用途に使用することができる。暗号乱数発生器は、暗号化、デジタル署名（非拒絶を含む）、専用通信プロトコル及びメッセージの保全性などのコンピュータセキュリティ用途により適していると考えられる。暗号乱数発生器は、電子通信の機密性、保全性、認証を強化及び保護するための基本構成単位である。対称暗号鍵又は非対称暗号鍵を生成するために暗号乱数発生器を使用することもできる。
【０００３】
通常、暗号乱数発生器は、クロック装置、或いはディスクドライブ、マウスの動き、キーボードの入力タイミング、実行処理、マイクのラインノイズのような内蔵ハードウェアから発生するその他のエントロピ源により生成(seed)され、これら全てを異なる組み合わせで置き換えて使用することもできる（ＩＥＴＦのＲＦＣ１７５０を参照のこと）。これらの生成源は、割り込み及びイベント処理などの特定のメカニズムにより効果が低下させらせ、またこれらのシステムに固有の期間（すなわち、反復前に出力される値の数）により制限を低下させてきた可能性がある。コンピュータシステムの主な構成要素は確定的な

ものであることが明確に意図されているため、これらを用いて真の乱数を発生させることはできない。

【０００４】

発生する乱数は、通常、所定の値の範囲における特定の確率、密度、及び分布を有する。暗号用途に適した理想的な乱数発生器は、無限の範囲にわたって均等に分布する非決定論的な値を提供することになると思われる。

【０００５】

ビデオ装置において擬似乱数を発生させる別の方法として、ビデオ受信装置を認証するための対称暗号化及び復号化処理で使用する暗号ビットの出力ストリームから擬似乱数を発生させるビデオソース及びシンク（受信）装置を含む公知の方法が存在してきた。この方法に基づくような乱数発生装置の１つの例が、米国特許出願公開第２００４１５６５００号に記載されている。

【０００６】

別の方法及び装置としては、欧州特許第１５４４７２６号Ａ１に記載されるように、熱雑音発生素子において発生する熱雑音、又は光に基づいてノイズを発生させる発光素子にさえも基づくアナログ乱数発生器を内蔵するものがある。関連する方法及び装置が、英国特許第２３９０２７１号に記載されている。最も一般的な方法は、ランダムの起点としてノイズ源を利用し、増幅器を利用してノイズに基づく波形を増幅し、クロック信号を使用して、この増幅したノイズ波形をアナログ－デジタル変換器でサンプリングしたときの間隔を示すことである。この方法では、真の乱数のシーケンスを発生させることができるが、アナログ乱数発生器のノイズ発生素子において障害が発生する状況がより多くなることが懸念される。このような障害は部分的なものに過ぎず、ノイズ波形の範囲を限定するだけの場合もある。装置は「ランダムな」数を出力し続けるため、この種の障害はすぐには明らかにならない場合がある。しかしながら、暗号システムにとって、このような状況は潜在的に極めて危険な状態となり得るものである。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】米国特許出願公開第２００４１５６５００号

【特許文献２】欧州特許第１５４４７２６号Ａ１

【特許文献３】英国特許第２３９０２７１号

【非特許文献１】ＩＥＴＦ　ＲＦＣ１７５０

【発明の概要】

【発明が解決しようとする課題】

【０００８】

従って、本発明の目的は、暗号乱数発生器にシードを与える処理、又は乱数を発生させる処理を改善することにある。

【課題を解決するための手段】

【０００９】

本発明の目的は、方法発明の独立請求項１及び２、並びに装置発明の独立請求項１３及び１４により達成される。好ましい実施形態については従属請求項で説明する。

【００１０】

詳細な例示の実施形態を参照しながら、以下本発明について説明する。多岐にわたる形式で本発明を具体化することができ、その一部は、開示される実施形態とは極めて異なる可能性があるということは明らかである。従って、本明細書で開示される特定の構造及び機能の詳細は代表的なものに過ぎず、本発明の範囲を限定するものではない。

【００１１】

本発明の１つの実施形態によれば、画像の少なくとも一部が入力されるが、複数の画像を使用することも可能である。次に、この画像の画素が選択され、その各々に関連する位置情報及び色情報が提供される。選択された画素に関連する位置情報及び色情報に基づい

て、所定数のビットが計算される。次に、これらのビットを用いて暗号乱数発生器にシード(seed)を与える。

【００１２】

ユーザが、自分で画像を選択及び／又は入力できることが望ましい。これにより、ユーザは、暗号乱数発生器にシード(seed)を与えるためのソースをいつでも変更し、かつユーザが取り出したい任意の画像を暗号乱数発生器に与えることさえもできるという独自の利点が与えられ、処理をより良好に制御できるようになる。

【００１３】

本発明の１つの実施形態では、装置のユーザが提供する印刷画像をスキャンするためにスキャナを含むことができる。これは、単に装置のユーザが乱数シード生成器に初期化用の画像入力を提供するためのメカニズムの１つである。このメカニズムにより、目標とする使い勝手、サイズ、及びコストに依存する装置を設計及び構築する際に柔軟性が与えられるようになる。

【００１４】

本発明の１つの実施形態では、装置のユーザが選択した時間及び場所において写真を撮影するためにカメラを含むことができる。これは、単に装置のユーザが乱数シード生成器に初期化用の画像入力を提供するためのメカニズムの１つである。

【００１５】

このメカニズムにより、目標とする使い勝手、サイズ、及びコストに依存した装置を設計及び構築する際に柔軟性が与えられるようになる。

【００１６】

本発明の１つの実施形態では、装置の内部に（ユーザが追加及び削除する）画像のリポジトリが保持される。これは、単に装置のユーザが乱数シード生成器に初期化用の画像入力を提供するためのメカニズムの１つである。このメカニズムにより、目標とする使い勝手、サイズ、及びコストに依存した装置を設計及び構築する際に柔軟性が与えられるようになる。

【００１７】

本発明の１つの実施形態では、シードの生成をサポートするために線形フィードバックシフトレジスタ（ＬＦＳＲ）が使用される。使用されるＬＦＳＲのサイズは、必要なシードのサイズに依存するため、（ＬＦＳＲ内のレジスタ素子の個数をｎとした場合）ｎビットのＬＦＳＲの構成を使用することができる。このＬＦＳＲの構成は、内部ＸＯＲ（タイプ１）又は外部ＸＯＲ　ＬＦＳＲ（タイプ２）、或いは両方のタイプの組み合わせであってもよい。

【００１８】

本発明の１つの実施形態では、シードの生成をサポートするために多入力シフトレジスタ（ＭＩＳＲ）が使用される。使用されるＭＩＳＲのサイズは、必要なシードのサイズに依存するため、（ＭＩＳＲ内のレジスタ素子の個数をｎとした場合）ｎビットのＭＩＳＲの構成を使用することができる。

【００１９】

スキャナ、カメラを通じて、或いは画像リポジトリからの選択によって供給される画像の成分の色及び位置が、ＬＦＳＲ又はＭＩＳＲへの入力として使用される。ＬＦＳＲ又はＭＩＳＲへの入力として画像の画素成分の各々及びすべてを使用することができ、これは場合によっては有用であり、望ましいことであるが、通常、エントロピにおける比例利得がなければ処理が遅くなるであろう。

【００２０】

クロックタイミング、前回の画素の色及び位置、画素を含む現在の行番号、又はシステムに固有の何らかの擬似ランダム変数源などの様々な基準に応じて無作為に選択された画像のランダムな画素成分の組みだけを使用することで最適化が行われる。これにより、さらに安全なシード(seed)の生成が行われる。

【００２１】

さらに、入力した画像のサイズ、色濃度、及び／又は色変化に基づいてこの画像の適合性を反映する良度指数を計算し、その後、計算された良度指数を、所望のセキュリティレベルなどに基づいて選択できる所定のしきい値と比較することは有利なことである。比較の結果、画像が適切でなければ、この画像は拒否され、及び／又は警告が出される。比較の結果、画像が適切であれば、この画像は受け入れられる。また後者の場合、ユーザに情報を与えることができる。この機能により、ユーザは、自身が入力した画像によって十分安全な鍵が届けられるであろうと確信できるようになる。それでもなお、ユーザは処理を完全に制御している。

【００２２】

画素サイズをＭＩＳＲ又はＬＦＳＲ内のレジスタ素子数と整合させること、すなわち３２ビットＭＩＳＲへ入力するために２５６ビット画素を３２ビット画素にダウンサイズすることで、別の最適化が行われる。さらなる処理の必要性又は要望がある場合、ＬＦＳＲ又はＭＩＳＲの入力（又は出力さえも）を機能回路に通すことも可能である。

【００２３】

ＬＦＳＲ又はＭＩＳＲからのｎビットの出力は、ｍビットのメモリバッファに蓄積されるが、この場合、ｍは必要な暗号シードのサイズであり、ＬＦＳＲ又はＭＩＳＲからのｎビットの出力の倍数である。メモリバッファへの様々な蓄積方法が実行可能である。オーバーフローする有効ビット値を破棄しながらＸＯＲ関数又は実に単純な算術の蓄積を用いて、後続するｍビットのメモリバッファに上記出力をラウンドロビン割り当てすることが可能である。

【００２４】

ほとんどの暗号乱数発生器は、固定サイズのシード(seed)を取り出すため、このシードにおけるエントロピの程度が、保護されるデータのセキュリティレベルに直接的に又は間接的に影響を与えることになる。本発明により、アプリケーションドメインのセキュリティレベル及び要件に応じて可変サイズのシードを使用することが可能となる。本発明により、装置のユーザが必要とする場合、新しい暗号シードの再生成も可能となる。

【００２５】

暗号乱数発生器にシード(seed)を与える代わりにエントロピを直接使用することも可能である。（さらなるテスト及び処理に依存する非対称鍵を例外とする）一部の暗号鍵に関しては、エントロピ源から鍵を直接生成することが可能であり、すなわち、暗号乱数発生器にシードを与えることなく、結果として生じるｍビットの暗号シードが暗号鍵として直接使用される。

【図面の簡単な説明】

【００２６】

【図１】従来技術の内部ｎステージの線形フィードバックシフトレジスタ（タイプ１ＬＦＳＲとも呼ばれる）の概略図である。

【図２】別の従来技術の外部ｎステージの線形フィードバックシフトレジスタ（タイプ２ＬＦＳＲとも呼ばれる）の概略図である。

【図３】従来技術の多入力シフトレジスタ（ＭＩＳＲ）の実施形態の概略図である。

【図４】本発明の１つの実施形態による暗号乱数シード生成システムの上位レベル図である。

【図５】本発明の画像処理ユニットのブロックフロー図である。

【発明を実施するための形態】

【００２７】

次に図面を参照しながら、本発明の１つの実施形態について説明する。図１は、本発明の１つの実施形態で使用される内部ｎステージの線形フィードバックシフトレジスタ（ＬＦＳＲ　タイプ１）を示す概略図である。図１のＬＦＳＲは、排他的論理和（ＸＯＲ）構成で組み合わされた出力を有するフリップフロップチェーンを含み、フィードバックメカニズムを形成する。各フリップフロップの出力は、レジスタ内を１つのビットから次の上位ビットへと進む。ＸＯＲを実行することによりフリップフロップの２又はそれ以上の出

力が共に組み合わされて、後続するフリップフロップの入力へ送り込まれる。ＲＥＳＥＴビットは、フリップフロップの各々への別の入力であり、フリップフロップの状態をリセット又はセットするために使用される。Ｎ個のフリップフロップのチェーンの出力が組み合わされて、ｎビットのＬＦＳＲの出力（Ｑ１からＱｎまで）を形成する。

【００２８】

図２は、本発明の別の実施形態において上述のように使用される外部ｎステージの線形フィードバックシフトレジスタ（ＬＦＳＲ　タイプ２）を示す概略図である。

【００２９】

図３は、本発明のさらに別の実施形態によるｎビットの多入力シフトレジスタ（ＭＩＳＲ）を示す概略図である。図３のＭＩＳＲに含まれるフリップフロップチェーンの出力は、排他的論理和（ＸＯＲ）構成で入力データビット（Ｄ１からＤｎ）と組み合わされ、チェーン内の次のフリップフロップへの入力として使用される。最後のフリップフロップの出力もまた、チェーン内の最初のフリップフロップへ戻される。ＲＥＳＥＴビットは、フリップフロップの各々への別の入力であり、フリップフロップの状態をリセット又はセットするために使用される。ＭＩＳＲ内のＮ個のフリップフロップのチェーンの出力が組み合わされて、ｎビットのＭＩＳＲの出力（Ｑ１からＱｎ）を形成する。

【００３０】

図４のブロック図では、カメラ２又はスキャナ４を使用して、暗号乱数のためのシード(seed)の生成において直接使用するための装置のユーザにより選択される画像１、又は複数の画像を提供する。このカメラ２又はスキャナ４を使用して画像１を提供し、リポジトリ３に格納することもでき、装置のユーザは、暗号乱数のためのシードの生成において使用する１又はそれ以上の画像をこのリポジトリから選択することができる。

【００３１】

図５のブロックフロー図には、ユーザがどのように画像１を選択するか、或いは画素の一部又は全てを選択する機能回路を通じて画像がどのように供給されるかについての例が示されている。選択ユニット５は、画素の処理すべきポジション値（画像サイズに基づくＸ、Ｙ軸）とカラー値（色空間及びビット深度のタイプによる）とを用いて特定のランダムな画素を抽出し、ｎビットのバッファデータとして生成し、畜積する。

【００３２】

選択された画素は、結果をＮビット（ｂ１からｂｎまで）で計算するために使用するポジション値（Ｘ、Ｙ）とカラー値（さらに精度をあげるために対応するビット深度を伴うグレースケール、ｒｇｂ、ｃｙｍ、ｈｓｂ、ｙｕｖ、又は可能な色空間の任意の組み合わせであってもよい）とを有することになる。ユーザが選択した画像１又は複数の画像のうちの選択された画素から、Ｎビットの結果を必要に応じて何度でも繰り返し計算することができる。何らかのしきい値を通過したサイズ、色濃度、及び色変化を有する画像１のみを受け入れることにより、ユーザが選択した画像１又は複数の画像の質をさらに高めることができる。別々に又は一度にこれらの特性を評価することができる。後者の場合、異なる特性を表す値に基づいて１つの値が計算される。同じ方法で、警告を出すか否かを決定することもできる。

【００３３】

さらに、画像を拒否し、及び／又は警告を出すために使用することができる各画像の（一方向ハッシュ関数により生成された）ハッシュを保持することにより、既に暗号乱数シードの生成に使用した画像の経過を追い、その後画像が再選択されることを防ぐことができる。

【００３４】

図４は、シフトレジスタの使用についての異なる２つの代替案を示す図である。図４では、左側に示されているオプションを選択して、各ビットをクロックサイクルごとにビットシフトすることにより、前のステップからの結果として生成されるＮビット（ｂ１からｂｎまで）が、図１又は図２のＬＦＳＲのＲＥＳＥＴビットへの入力として使用される。ブロック図は、最上位ビット（ｍｓｂ）のビットシフトを示しているが、ＬＦＳＲのＲＥ

ＳＥＴビットへの入力として最下位ビット（ｌｓｂ）をビットシフトすることも十分可能である。これらのビットのうちの任意のビットをＬＦＳＲのＲＥＳＥＴビットへの入力として使用することができる。前のステップからの結果として生じる次のＮビットは、ＬＦＳＲのＲＥＳＥＴビットへのさらなる入力として使用される。ＬＦＳＲの各クロックサイクルは、Ｎ個の出力ビット（Ｑ１からＱｎまで）を生成して、暗号乱数発生器のためのｍ×ｎビットのシード(seed)として畜積する（この場合、ｍは、必要なシードのビット数を決定するために使用される任意の倍数であり、整数である）。

【００３５】

本発明の別の実施形態が、図４の右側にブロック図として示されており、上述の機能回路により結果として生成されたＮビット（ｂ１からｂｎまで）がｎビットのＭＩＳＲへの入力として使用され、（図では最上位ビットに印が付いているが）これらのビットのうちの任意のビットが各クロックサイクルにおいてＭＩＳＲのＲＥＳＥＴビットへの入力として使用される。全てのＮビット（ｂ１からｂｎまで）がＭＩＳＲへの入力（Ｄ１からＤｎまで）として同時に使用される。ＭＩＳＲの各クロックサイクルは、Ｎ個の出力ビット（Ｑ１からＱｎまで）を生成して、暗号乱数発生器のためのｍ×ｎビットのシード(seed)として畜積する（この場合ｍは、必要なシードのビット数を決定するために使用される任意の倍数である）。

【００３６】

添付の請求項に記載されるような本発明の範囲内で様々な変更及び修正を行うことができるため、本発明は上述の実施形態に限定されるものではない。従って、本発明の技術範囲内にはこのような変更及び修正が含まれることも意図されている。

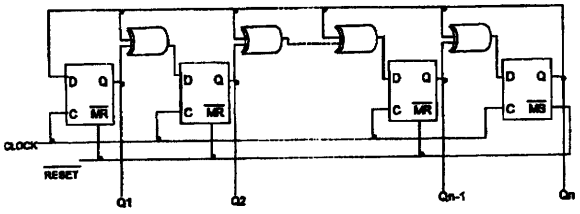
【符号の説明】

【００３７】

１　画像
２　カメラ
３　リポジトリ
４　スキャナ
５　関数

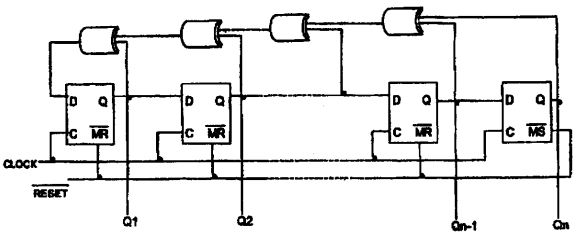
【図１】

内部nステージの線形フィードバックシフトレジスタ LFSR(タイプ1)



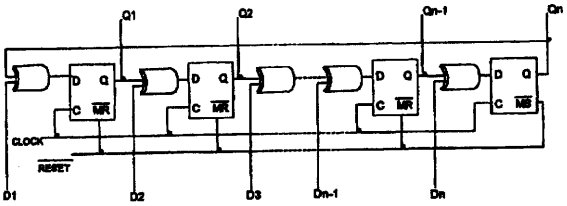
【図２】

外部nステージの線形フィードバックシフトレジスタ LFSR(タイプ2)



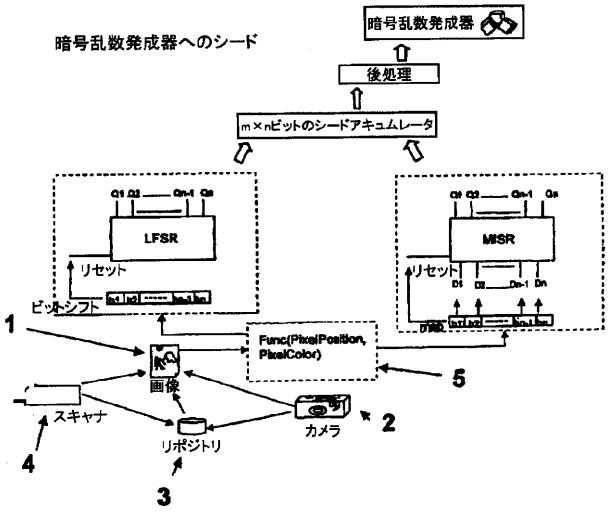
【図３】

多入力シフトレジスタ MISR



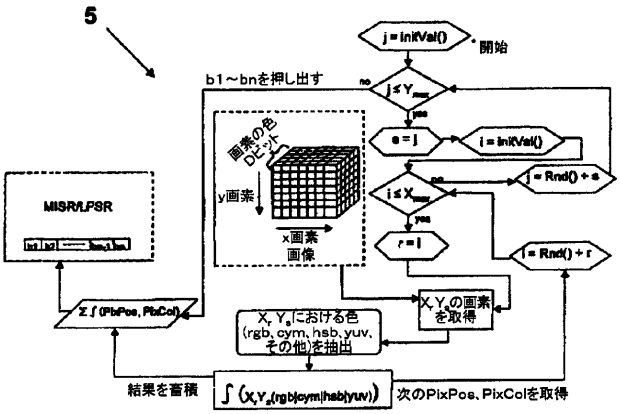
【図４】

暗号乱数発成器へのシード



【図５】

Func(PixelPosition, PixelColor)



【手続補正書】
【提出日】平成25年8月7日(2013.8.7)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
暗号乱数発生器を備えた装置において前記暗号乱数発生器にシード(seed)を与えるための方法であって、前記装置において、
画像（１）の少なくとも一部を入力するステップと、
前記画像（１）の画素を選択するステップであって、該画素の各々には関連する位置及び色の情報が与えられており、現在選択された画素の色及び位置の少なくとも１つに基づき次の画素の選択を繰り返すことにより適合性を満たす画像のみを受け入れ、その結果、乱数値を生成するのに適した前記画像（１）の画素の部分集合がランダムに選択される当該ステップと、
前記ランダムに選択された画素に関連する前記位置及び色の情報を用いて所定数のビットを計算するステップと、
前記暗号乱数発生器にシードを与えるために、前記計算された数のビットを出力するステップと、
が実行されることを特徴とする方法。
【請求項２】
暗号乱数発生器により暗号乱数を発生させるための方法であって、前記暗号乱数発生器が、
画像（１）の少なくとも一部を入力するステップと、
前記画像（１）の画素を選択するステップであって、該画素の各々は関連する位置及び色の情報が与えられており、現在選択された画素の色及び位置の少なくとも１つに基づき次の画素の選択を繰り返すことにより適合性を満たす画像のみを受け入れ、その結果、乱数値を生成するのに適した前記画像（１）の画素の部分集合がランダムに選択される当該ステップと、
前記ランダムに選択された画素に関連する前記位置及び色の情報を用いて所定数のビットを計算するステップと、
前記計算された数のビットを暗号乱数として出力するステップと、
を実行することを特徴とする方法。
【請求項３】
前記入力するステップは、後のステップで使用される複数の画像（１）を入力するステップを含む、
ことを特徴とする請求項１又は２の何れか１項に記載の方法。
【請求項４】
前記入力するステップは、
前記入力された画像のサイズ、色濃度、及び色変化の少なくとも１つに基づいてこの画像の前記適合性を反映する良度指数を計算するステップと、
前記計算された良度指数を所定のしきい値と比較するステップと、
前記比較の結果、前記画像（１）が適切でなければ、拒否するか、或いは警告を出すステップと、
前記比較の結果、前記画像（１）が適切であれば、前記画像（１）を受け入れるステップと、
をさらに含むことを特徴とする請求項１～３の何れか１項に記載の方法。
【請求項５】

既に使用された画像を拒否する及び警告の少なくとも１つを出すことにより、画像の再選択を防止する、
ことを特徴とする請求項４に記載の方法。
【請求項６】
前記所定数のビットを計算する前記ステップは、線形フィードバックシフトレジスタ又は多入力シフトレジスタを使用する、
ことを特徴とする請求項１～５の何れか１項に記載の方法。
【請求項７】
前記画像（１）の画素を選択する前記ステップは、画素サイズをレジスタ素子数と整合するステップをさらに含む、
ことを特徴とする請求項１～６の何れか１項に記載の方法。
【請求項８】
前記所定数のビットを計算する前記ステップは、ビットをバッファすることにより前記所定数の出力ビットを変更できるようにするステップを含む、
ことを特徴とする請求項１～７の何れか１項に記載の方法。
【請求項９】
暗号乱数発生器にシード(seed)を与えるための装置であって、
画像（１）の少なくとも一部を入力するように構成された入力手段と、
前記画像（１）の画素を選択するように構成された選択手段（５）であって、該画素の各々には関連する位置及び色の情報が与えられており、現在選択された画素の色及び位置の少なくとも１つに基づき次の画素の選択を繰り返すことにより適合性を満たす画像のみを受け入れ、その結果、乱数値を生成するのに適した前記画像（１）の画素の部分集合がランダムに選択される当該選択手段と、
前記ランダムに選択された画素に関連する前記位置及び色の情報を用いて所定数のビットを計算するように構成された計算手段と、
前記暗号乱数発生器にシードを与えるために、前記計算された数のビットを出力するように構成された出力手段と、
を備えることを特徴とする装置。
【請求項１０】
暗号乱数を発生させるための装置であって、
画像（１）の少なくとも一部を入力するように構成された入力手段と、
前記画像（１）の画素を選択するように構成された選択手段（５）であって、該画素の各々には関連する位置及び色の情報が与えられており、現在選択された画素の色及び位置の少なくとも１つに基づき次の画素の選択を繰り返すことにより適合性を満たす画像のみを受け入れ、その結果、乱数値を生成するのに適した前記画像（１）の画素の部分集合がランダムに選択される当該選択手段と、
前記選択された画素に関連する前記位置及び色の情報を用いて所定数のビットを計算するように構成された計算手段と、
前記ランダムに計算された数のビットを暗号乱数として出力するように構成された出力手段と、
を備えることを特徴とする装置。

フロントページの続き

(72)発明者　ブサリ　ジェイ
タイ　１０５００　バンコク　バンラック　シロム　ロード　１７４　ビルディング　セカンド　フロア　クリプトグラフ　カンパニー　リミテッド内

Ｆターム(参考) 5C075 CD20 CD22 EE03
5J104 FA01 NA04