(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
H04L 9/20 (2006.01)
H04L 9/32 (2006.01)
G06F 7/58 (2006.01)

(11) 공개번호 10-2007-0021987
(43) 공개일자 2007년02월23일

(21) 출원번호 10-2006-7005917
(22) 출원일자 2006년03월24일
심사청구일자 없음
번역문 제출일자 2006년03월24일
(86) 국제출원번호 PCT/EP2004/052861
국제출원일자 2004년11월08일
(87) 국제공개번호 WO 2005/050434
국제공개일자 2005년06월02일

(30) 우선권주장 03 13491 2003년11월18일 프랑스(FR)

(71) 출원인 아뜨멜 그르노블
프랑스 에프-38120 생 에그르브 아브뉘 드 로슈쁠렌느

(72) 발명자 메니앙 쟝-프랑수와
프랑스 38100 그르노블 7 알레 뒤 팍 쥐. 폼피두
프랑시올리 파브리스
프랑스 74890 봉 앙 샤블레 루트 데 샤르모뜨 당 오뜨

(74) 대리인 특허법인코리아나

전체 청구항 수 : 총 9 항

(54) 랜덤 이진 시퀀스 생성기

(57) 요약

본 발명은 랜덤 이진 또는 숫자 시퀀스의 생성에 관한 것이다.

본 발명에 따르면, 시퀀스는 지문 센서 (10) 및 아날로그-디지털 변환기 (14) 로 부터 생성된다. 랜덤 이진 시퀀스는 (낮은 순서 비트를 랜덤하게 동작시키기 위해 센서로부터 신호의 잡음 레벨에 대한 충분한 정밀 해상도를 가진) 변환기로부터의 낮은 순서 비트에서 생성된다. 상기 센서는 초전성 검출기의 매트릭스인 것이 바람직하다. 비트의 순서는 재구성 회로에 의해 스크램블되고, 수단 (18) 은 생성된 시퀀스 내에서 0 및 1 비트의 분배의 균형을 위해 제공된다.

대표도

도 1

특허청구의 범위

청구항 1.

물리적으로 발신된 랜덤 시퀀스를 생성하기 위한 주성분으로서, 개별 검출기의 매트릭스를 갖는 지문 센서 (10) 를 포함하고,

상기 센서는 개별 검출기에 의해 검출된 상기 전압 레벨을 디지털 형태로 변환하기 위한 아날로그-디지털 변환기 (14) 를 포함하며,

유사-랜덤 시퀀스의 상기 비트를 형성하기 위해 상기 변환의 상기 낮은 순서 가 이용되는, 랜덤 이진 시퀀스 생성기.

청구항 2.

제 1 항에 있어서,

상기 개별 검출기가 초전성 셀인 것을 특징으로 하는 랜덤 이진 시퀀스 생성기.

청구항 3.

제 1 항 또는 2 항에 있어서,

상기 센서는 스캐닝 센서이고,

다수의 검출기의 몇몇 열 (row) 들로 이루어진 매트릭스는, 손가락이 상기 센서의 표면 위를 스칠 때 지문을 검출하도록 이용되는, 랜덤 이진 시퀀스 생성기.

청구항 4.

제 1 항 내지 3 항 중 어느 한 항에 있어서,

상기 시퀀스의 상기 랜덤 특성을 강화하기 위하여, 상기 비트의 순서를 스크램블 (scramble) 하는 수단을 포함하는 것을 특징으로 하는, 랜덤 이진 시퀀스 생성기.

청구항 5.

제 4 항에 있어서,

0 비트 및 1 비트의 보다 나은 분배를 가지는 시퀀스를 형성하기 위하여, 상기 00 쌍 및 11 쌍을 제거하고, 01 쌍을 제 1 비트로 변환하고 10 쌍을 반전 비트로 변환하기 위한, 낮은 순서 비트의 연속적인 쌍을 샘플링하기 위한 수단을 포함하는 것을 특징으로 하는, 랜덤 이진 시퀀스 생성기.

청구항 6.

제 5 항에 있어서,

상기 변환이 01 및 10 쌍의 2 개의 연속적인 시리즈 사이에서 반전하고, 제 1 변환은 상기 01 쌍을 0 비트로 매핑 (mapping) 하고, 반전 변환은 상기 10 쌍을 1 비트로 매핑하는 것을 특징으로 하는, 랜덤 이진 시퀀스 생성기.

청구항 7.

제 6 항에 있어서,

상기 변환은 비트의 새로운 쌍 각각 상에서 반전되는 것을 특징으로 하는, 랜덤 이진 시퀀스 생성기.

청구항 8.

제 1 항 내지 7 항 중 어느 한 항에 있어서,

상기 지문의 이미지를 검증하는 수단을 포함하고, 상기 수단은 특히 상기 다양한 개별 검출기로부터의 신호 값의 표준 편차 및/또는 상기 수단의 값을 검증하는 수단을 포함하는, 랜덤 이진 시퀀스 생성기.

청구항 9.

제 1 항 내지 제 8 항 중 어느 한 항에 있어서,

지문 센서에 의해 검출된 지문을 암호화하는 수단을 포함하고,

상기 암호화 수단은 상기 랜덤 시퀀스 생성기를 이용하는, 랜덤 이진 시퀀스 생성기.

명세서

발명의 배경

본 발명은 주로 암호 애플리케이션에 이용되는 랜덤 (무작위; random) 숫자 혹은 이진 시퀀스 (binary sequence) 에 관한 것으로: 많은 암호화 소프트웨어 패키지는 가능한 한 랜덤인 키의 생성을 요구한다.

순수 알고리즘 랜덤수는 사실상 유사-랜덤수 생성기 (pseudo-random number generator) 이며; 랜덤인 것처럼 보이지만 전체적으로 랜덤하지 않은 보다 많은 또는 보다 적은 시퀀스의 랜덤 특성을 측정하기 위하여 이용된 테스트에서 증명된 바와 같이, 이러한 수들은 충분히 랜덤하지 못하다.

이진 시퀀스를 보다 랜덤하게 하기 위해, 오퍼레이터로 하여금 전기적으로 기록된 랜덤 동작을 수행하는 것, 예를 들어, 마우스에 의한 임의의 수동 동작을 생성하기 위하여, 암호 소프트웨어 패키지의 랜덤수 생성이 사용자가 요청하는 단계, 컴퓨터에 앉는 단계로 이루어지는 것을 요구하는 인간 오퍼레이터의 개입이 이미 제안되었으며, 이러한 전기적으로 기록된 랜덤 동작들은 랜덤 시퀀스를 정의하도록 기록되고 요구된다. 그러나, 이러한 시퀀스는 여전히 충분히 랜덤하지 못하는 것을 경험을 통하여 나타낸다.

열 잡음과 같이, 랜덤 이벤트 (event) 의 물리적 소오스에 기초한 규칙적인 생성기들이 있다. 이 물리적 소오스는 이 물리적 소오스를 랜덤 시퀀스로 변환시켜 주는 포매팅 (formatting) 회로에 적용된다. 불행히도 이러한 생성기는 통계적으로 매우 양호하지 않은데, 이는 상관관계가 자주 나타나고, 외부 조건에 연관되어 있기 때문이며; 예를 들어, 장비에 전력을 공급하기 위해 사용된 전기 네트워크의 50 Hz 혹은 60 Hz 주파수는 전자회로 내의 잔여물 형성에 영향을 미치며, 예측 랜덤 시퀀스에서 명확하게 비-랜덤 성분을 생성하기 때문이다.

또한 유사-랜덤 생성기 및 랜덤 물리 소오스의 결합을 관찰할 수 있는데, 이 물리 소오스는 시퀀스의 비트를 생성하는 프로세스를 인계하는 유사-랜덤 생성기를 시작하기 위한 " 시드 (seed)" 를 생성한다. 그러나, 다음으로 물리 소오스와 유사-랜덤 생성기 사이의 결합을 획득하기 위해 비교적 복잡한 시스템의 사용이 필요하다.

본 발명의 목적은 물리 소오스에 기초하여 본질적으로 강한 랜덤 특성 (nature) 을 나타내고, 생성된 비트의 시퀀스가 대부분의 통계학적 테스트 관점에서 이미 만족 되었기 때문에 유사-랜덤 생성기를 요구하지 않거나 또는 실제적으로 요구하지 않는 새로운 타입의 랜덤 생성기를 제안하는데 있다.

본 발명은 물리적으로 발신된 랜덤 시퀀스를 생성하기 위한 주성분으로서, 개별 검출기의 매트릭스를 가진 지문 센서를 포함하고, 이 센서는 개별 검출기에 의해 검출된 전압 레벨을 디지털 형태로 변환하기 위한 아날로그-디지털 변환기를 포함하는 센서, 유사-랜덤 시퀀스의 비트를 형성하기 위해 이용되는 이 변환의 낮은 순서 비트를 포함하는 랜덤 시퀀스 생성기를 제안한다.

센서는 스캐닝 센서이고, 다수의 검출기의 몇몇 열로 이루어진 매트릭스가 손가락이 센서의 표면을 스칠 때 지문을 검출되도록 이용된다. 이러한 센서는 프랑스 특허출원공개 FR-A-2 749 955 에 개시된다.

이 센서는 개별 검출기의 내부가 초전성 셀 (pyroelectric cell) 인 센서인 것이 바람직하다.

랜덤 생성기로서 지문 센서의 이용은 특히 타겟 애플리케이션 (특히 암호 애플리케이션) 이 안전한 환경에서 작동하도록 의도되고 지문 센서가 특히 보안을 위해 추천된다는 사실로 나타난다. 그러므로 지문 인식 보안 기능 및 랜덤 신호 생성 기능은 보안의 다른 종류 (특히, 암호에 의한 보안) 를 위해 싱글 센서를 이용하여 편리하게 결합된다. 좀 더 나아가, 본 발명은 (암호로의 전송, 인식 및 인증 시스템 이전에) 지문 그 자체가 암호화되는 것을 가능하게 하며 , 지문은 지문을 암호화하기 위해 이용되는 랜덤 시퀀스를 생성하기 위해 그 자체가 판독되어 이용된다.

보다 바람직하게, 아날로그-디지털 변환기로부터의 낮은 순서 비트의 순서는 인접 검출기들 (혹은 픽셀 (picxel)) 혹은 인접 열 (row) 들 사이에서 상관관계를 제한하기 위해 스크럼블링된다.

본 발명의 다른 기능 및 이점은 첨부 도면을 참조하여 다음의 상세 기술을 읽음으로써 명백해지며, 이 기술 내의 단일 (single) 수치는 본 발명에 따른 랜덤 시퀀스 생성기를 나타낸다.

개별 초전성 검출기는 신호를 증폭하는 읽혀진 신호에 접속된 개별 커패시터를 형성하는 세라믹 초전성 (또는 압전기 (piezoelectric), 등에 상당하는) 층 또는 PVDF (polyvinylidene fluoride) 와 같은 플라스틱 또는 세라믹으로 형성된다. 다음으로 이 신호는 변환기에 의해 디지털 형태로 변환된다. 열 (row) 내의 다양한 검출기 및 픽셀로부터의 신호는 순차적으로 판독되고 또한 다양한 열로부터의 신호가 순차적으로 판독된다.

손가락이 센서에 닿지 않을 때, 검출기가 견디는 외부 온도 및 집적 회로 칩의 전력 손실을 고려하여, 각 픽셀은 이 환경에서 대략 열 균형을 이룬다.

그러나, 초전성 층은 외부 장애에 극도로 민감하며; 공기의 흡입, 잡음, 진동이 전하 (charge) 레벨을 쉽게 변경할 수 있으므로, 신호의 레벨이 판독되고 변환된다. 이에 전자적 잡음이 더해진다. 이러한 장애는 손가락의 존재에 의한 주 신호의 부재상태에서 존재하지만, 이들은 이것이 존재할 때 메인 신호에 더해진다.

랜덤 잡음 소오스는 주 신호의 부재 혹은 존재 상태에서 아날로그-디지털 변환기의 최소의 현저한 비트에 의해 형성된다. 또한, 이것은 지문을 판독하는 것에 관한 문제이기 때문에 많은 다양한 픽셀들이 이용되며, 이러한 픽셀로부터의 신호들은 이들이 병렬로 정렬되지 않을 때에도 그들과 그 이상 사이에서 광범위하게 상관관계가 끊어진다.

도면은 본 발명에 따른 시스템을 나타낸다. 지문 센서 (10) 는 단면도에 나타나며; 이는 그 상부에 손가락이 놓여 지거나 스쳐질 수 있는 영역 (10) 내에 초전성 커패시터의 매트릭스를 포함하는 실리콘 칩이다. 칩은 매트릭스를 어드레싱하고, 매트릭스로부터의 신호를 판독하고, 증폭하고, 아날로그-디지털 변환을 제공하는 그 자신의 수단을 가진다. 이러한 수단은 표현의 더 큰 용이함을 위해 칩 외부에 도시된다.

예를 들면, 매트릭스는 각각 8 열의 280 픽셀을 포함하며, 1 밀리초 (millisecond) 마다 주기적으로 판독된다. 판독된 신호는 증폭되고 변환기에 의해 디지털 형태로 변환된다. 4-비트 해상도를 가진 변환기는 지문 이미지를 취하는데 충분하지만, 최소의 현저한 비트의 랜덤 특징을 강화하기 위해 좀 더 높은 해상도 변환기가 제공될 수 있다.

일반적인 규칙으로서, 시스템 디자인에서, 판독된 신호의 증폭 레벨은 자연 잡음 (열, 전기 등) 이 후반부가 랜덤하게 움직이는데 최소의 현저한 비트의 레벨보다 크게 되는 것이 충분하도록 모든 노력이 행해진다.

이것은 비트의 랜덤 시퀀스를 형성하기 위해 이용된 아날로그-디지털 변환기 (14) 의 출력시 최소의 현저한 비트이다.

그러나, 시퀀스는 변환기 (14) 의 출력시 직접적으로 샘플링되지 않는 것이 바람직하다. 더 정확히 말하면, 이는 픽셀 재구성 회로 (16) 의 출력에 취해지는 것이 바람직하다. 또한, 재구성 회로 (16) 는 지문 센서 칩 상에 위치한다.

재구성 회로 (16) 는 매트릭스의 행 (column) 의 순서대로, 열 (row) 내에서 열 대 열로, 지문 검출 매트릭스의 어드레싱 순서로 도착하는 변환기 (14) 로부터의 낮은 순서 비트들을 차례로 취한다. 재구성 회로 (16) 는 변환기로부터 수신된 비트의 순서를 스크램블링함으로써, 매트릭스 내의 인접 픽셀으로부터의 비트가 랜덤 시퀀스의 순서에 인접하지 않게 된다. 이는 시퀀스 내의 상관관계를 회피한다.

임의의 경우, 재구성 회로의 기능은 인접 픽셀 사이의 상관관계, 다른 상관관계, 또는 공지된 상관관계의 대부분을 제거하는 것이다. 예를 들어, 재구성 회로는 매트릭스의 열 (row) 의 숫자로부터 동일한 행 및 그 비트가 연속적으로 통과하는 것을 허용하지 않도록 한다. 실제로, 이들은 상이한 순간에 동일한 이미지를 보는 것이 필요하기 때문에 상이한 열 (row) 들 사이에는 상관관계가 이론적으로 있다.

또한, 재구성 회로 다음으로 비트의 평균 배분을 조절하기 위한 회로 또는 소프트웨어 수단 (18) 이 후속하는데, 평균 기간을 초과하여, 시퀀스는 1 비트가 있는 것만큼 0 비트도 많이 포함해야 한다. 이는 비교적 간단한 알고리즘에 의해 행해진다. (픽셀의 순서가 스크램블링됨으로써 결정되는) 첫 번째 재구성으로부터의 비트는 2 개로 판독된다. 비트들이 둘 다 0 이거나 또는 둘 다 1 일 때, 그들은 매우 간단하게 무시된다. 첫 번째가 0 에 있고, 두 번째가 1 에 있을 때는, 1 비트가 생성된다; 반대인 경우에는, 0 비트가 생성된다 (또는, 당연히 반대도 가능하다).

이는, 적어도 첫 번째 근사값으로서, 1 비트가 있는 것만큼 많은 0 비트를 획득하는 것을 가능하게 하는데, 그 이유는 만약 랜덤 소오스가 부정확하게 배분되고, 1 비트보다 많은 0 비트를 발생하면 (예를 들어) 이 경우 결합 00 이 통계적으로 좀 더 빈번하게 나타나야 하고 결합 11 은 보다 적게 나타나야만 하기 때문이다. 이 두 결합이 제거되기 때문에, 단지 다른 두 개만 남게 되고, 남은 두 개가 비정상으로 분배될 이유는 없다.

그러나 분배가 여전히 비정상적인 경우, 위의 변환이 주기적으로 교대해야 바람직하고; 그러므로, 수신된 일련의 쌍, 01 혹은 10 에 대하여, 변환이 01 을 1 비트로 변환하고 10 을 0 비트로 변환하지만, 후속하는 시리즈의 쌍에 대해서는, 변환이 01 을 0 비트로 변환하고 10 을 1 비트등으로 변환한다. 이 변환은 각 쌍에서 교대될 수도 있으며, 즉, 생성된 랜덤 시퀀스의 각 비트를 반전한다.

연속적인 비트의 쌍을 생성시키기 위한 픽셀의 선택은 상관관계를 회피하도록 재구성 회로에 의해 행해지고, 각각의 쌍에 대해, 멀리 떨어져 분리된 픽셀의 한 쌍을 이용하는 것이 이롭게 제안되는데; 예를 들어 매트릭스 열 (row) 의 왼쪽 말단에 있는 픽셀은 열의 중간에 있는 픽셀과 동시에 착출되며, 다음으로 새로운 쌍, 즉, 중간으로부터 시작한 두 번째 픽셀과 함께 왼쪽에서부터 시작한 두 번째 픽셀, 등을 착출하기 위해 하나의 스텝 (step) 을 왼쪽으로 이동 (shift) 한다.

다른 가능성은 가능하다고 증명된 상관관계를 회피하기 위한 원칙이 제공될 수 있다.

만약 랜덤 시퀀스가 빠른 발생을 요구하지 않으면, 열 (row) 내의 모든 픽셀의 이용은 각 이미지의 라인 스캔 (line scan) 에 이용된 픽셀의 그룹을 변경함으로써 그들의 오직 몇몇만을 이용하여 회피할 수 있다. 이것은 (속도의 손실에서, 좀 더 많은 라인이 동일한 랜덤 시퀀스 길이를 필요로 하기 때문에) 랜덤 특성 (nature) 을 증가시킨다.

임의의 외부의 비논리적인 (spurious) 영향에 대항하는 랜덤 시퀀스 생성기를 보호하기 위해, 정확한 동작의 체크 (check) 에 이용되는 회로 및 주기적 셀프-테스트 소프트웨어의 형식으로 제어회로 혹은 소프트웨어 (20) 가 더해지는 것이 바람직하다. 셀프-테스트는 지문 픽셀로부터 신호값의 분배의 주기적인 증명에 의존한다. 이는 대게 센서의 포화를 초래할 수 있도록 0 도 아니어야 하고 매우 높지도 않아야 하는 이미지 이상으로 신호의 수단을 계산함으로써 행해질 수 있다. 또한, 표준 편차 계산은 다양한 픽셀로부터의 신호값들 사이에서 수행될 수 있으며; 표준 편차는 너무 낮지도 (픽셀이 동일한 신호 레벨을 제공해야만 하는 이유는 없다) 않고 너무 높지도 않은 (비정상적인 것이 센서에서 동작하는 것을 표현하는) 않은 값을 가져야 한다. 또한 값들의 막대그래프를 (막대 그래프에서 갭 (gap) 의 부재 혹은 불연속을 체크하는) 모니터를 할 수 있다.

마지막으로, 픽셀의 값들이 시간에 따라 변화하는 것은 체크할 수 있는데, 즉, 센서에 의해 판독되는 동일한 이미지 패턴 (the same image pattern) 은 항상 아닌 것을 체크할 수 있다.

이는 이미지에 어떤 "소멸된 (dead)" 픽셀이 없다는 것을 체크할 수 있으며, 만약 있다면, 랜덤 시퀀스 생성 프로세스로부터 제거된다.

비록 본 발명에 따른 바람직한 지문 센서는 초전성 셀 센서이지만, 용량성 센서 또는 광센서에도 적용 가능하다. 극단적인 경우, 유사-랜덤 시퀀스 (pseudo-random sequence)를 생성하기 위해, 매트릭스의 전부가 아닌 단지 싱글 검출 셀 만을 이용하는 것이 가능하지만, 본 실시형태에서는 염두해 두지 않는다.

앞서 설명된 랜덤 시퀀스 생성기는 암호화 수단을 이용하는 시스템에서 특히 유용하다. 특히, 지문의 암호 수단은 지문 센서에 의해 검출되었다. 다음으로 지문 기록은 이 지문의 전송을 암호화하기 위해 이용된 유사-랜덤 시퀀스의 생성을 위해 차례로 이용된다.

도면

도면1