(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0026828
(43) 공개일자 2012년03월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01)
(21) 출원번호 10-2010-0088979
(22) 출원일자 2010년09월10일
심사청구일자 2010년09월10일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
홍석희
서울특별시 도봉구 마들로 859-19, 한신아파트 103동 107호 (도봉동)
김희석
서울특별시 강서구 화곡5동 스카이뷰 102동 507호
김민수
서울특별시 노원구 화랑로51길 17, 화랑타운 711동 501호 (공릉동)
(74) 대리인
특허법인충현

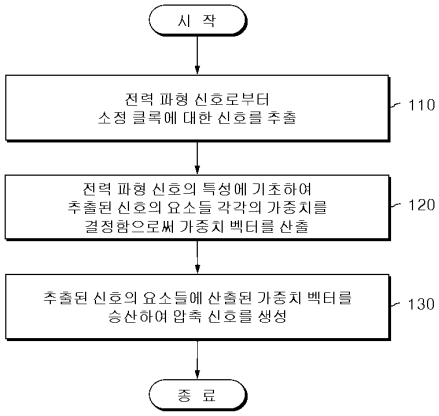
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **전력 분석 공격을 위한 신호 압축 장치 및 방법**

(57) 요 약

본 발명은 전력 분석 공격을 위한 신호 압축 장치 및 방법에 관한 것으로, 본 발명에 따른 신호 압축 방법은 전력 파형 신호로부터 적어도 하나 이상의 특정 클록에 대한 신호를 추출하고, 추출된 신호의 요소들 각각의 가중치를 전력 파형 신호의 특성에 기초하여 결정함으로써 가중치 벡터를 산출하며, 추출된 신호의 요소들에 산출된 가중치 벡터를 승산함으로써 압축된 신호를 생성한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

전력 분석 공격을 위한 신호 압축 방법에 있어서,

전력 파형 신호로부터 적어도 하나 이상의 소정 클록(clock)에 대한 신호를 추출하는 단계;

상기 전력 파형 신호의 특성에 기초하여 상기 추출된 신호의 요소들 각각의 가중치를 결정함으로써 가중치 벡터(weight vector)를 산출하는 단계; 및

상기 추출된 신호의 요소들에 상기 산출된 가중치 벡터를 승산하여 압축 신호를 생성하는 단계를 포함하는 방법.

청구항 2

제 1 항에 있어서,

상기 가중치 벡터를 산출하는 단계는 주성분 분석(PCA)을 이용하여 상기 추출된 신호의 요소들에 대한 압축 신호의 분산이 최대가 되도록 가중치 벡터를 결정하는 것을 특징으로 하는 방법.

청구항 3

제 1 항에 있어서,

상기 가중치 벡터를 산출하는 단계는 상기 전력 파형 신호의 변동이 큰 신호에 상대적으로 더 큰 가중치를 부여하는 것을 특징으로 하는 방법.

청구항 4

제 1 항에 있어서,

상기 가중치 벡터를 산출하는 단계는,

상기 추출된 신호의 요소들로부터 공분산 행렬(covariance matrix)을 산출하는 단계;

산출된 공분산 행렬로부터 고유 벡터들과 고유 값들을 산출하는 단계;

산출된 고유 값들 중 상대적으로 값이 큰 고유 값들에 대응하는 소정 개수의 고유 벡터들을 선택하는 단계; 및

상기 선택된 고유 벡터들을 가산하여 가중치 벡터를 산출하는 단계를 포함하는 방법.

청구항 5

제 4 항에 있어서,

상기 고유 벡터들을 선택하는 단계는 상기 전력 파형 신호와 상관도가 낮은 고유 벡터를 소거함으로써 수행되는 것을 특징으로 하는 방법.

청구항 6

제 1 항에 있어서,

상기 산출된 가중치 벡터를 이용하여 상기 전력 파형 신호의 모든 클록에 대한 압축 신호를 생성하는 단계를 더 포함하는 방법.

청구항 7

제 1 항에 있어서,

상기 전력 파형 신호의 클록들 각각에 대해 상기 가중치 벡터를 산출하는 단계 및 상기 압축 신호를 생성하는 단계를 반복하여 수행하는 단계를 더 포함하는 방법.

청구항 8

제 1 항 내지 제 7 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 9

전력 분석 공격을 위한 신호 압축 장치에 있어서,

전력 파형 신호를 입력받는 입력부; 및

상기 입력된 전력 파형 신호로부터 적어도 하나 이상의 소정 클록에 대한 신호를 추출하고, 상기 전력 파형 신호의 특성에 기초하여 상기 추출된 신호의 요소들 각각의 가중치를 결정함으로써 가중치 벡터를 산출하고, 상기 추출된 신호의 요소들에 상기 산출된 가중치 벡터를 승산하여 압축 신호를 생성하는 신호 처리부를 포함하는 장치.

청구항 10

제 9 항에 있어서,

상기 가중치 벡터는 주성분 분석을 이용하여 상기 추출된 신호의 요소들에 대한 압축 신호의 분산이 최대가 되도록 하는 값으로 결정되는 것을 특징으로 하는 장치.

청구항 11

제 9 항에 있어서,

상기 신호 처리부는,

상기 추출된 신호의 요소들로부터 공분산 행렬을 산출하고,

산출된 공분산 행렬로부터 고유 벡터들과 고유 값들을 산출하고,

산출된 고유 값들 중 값이 큰 고유 값들에 대응하는 소정 개수의 고유 벡터들을 선택하고,

상기 선택된 고유 벡터들을 가산함으로써 가중치 벡터를 산출하는 것을 특징으로 하는 장치.

명 세 서

기 술 분 야

[0001] 본 발명은 암호화 통신에 대한 부채널 공격 방법인 전력 분석 공격을 위한 신호 압축 장치 및 방법에 관한 것으로, 특히 전력 분석 공격을 위한 신호 처리 과정에서 전력 신호의 특성을 고려하여 신호를 압축하는 장치, 방법 및 이를 기록한 기록매체에 관한 것이다.

배 경 기 술

[0002] 기밀을 요구하는 정보를 안전하게 상대방에게 전달하기 위해 많은 학자들은 정보의 암호화 및 복호화 방법에 대해 연구하여 왔고, 현대 암호는 통신에 있어서 무결성, 기밀성 및 인증을 통해 통신의 안전성을 제공할 수 있게 되었다. 그러나, 수학적으로 안전한 것으로 알려진 알고리즘조차도 구현 단계에서 고려되지 못한 부가적인 정보의 누출이 있다는 것이 알려졌고, 이러한 약점으로부터 비밀 정보를 획득할 수 있는 부채널 공격(side channel attack)이 소개되었다. 부채널 공격은 통신상의 실행시간, 전력 소비, 전자기파 방사 등의 물리적 특성을 측정하고 통계적 기술을 이용함으로써 암호화된 정보 내에 포함된 비밀 키(key)에 관련된 정보를 부채널(side channel)로부터 획득한다.

[0003] 이러한 부채널 공격에는 오류 주입 공격(fault insertion attack), 시간 공격(timing attack), 전력 분석 공격(power analysis attack) 및 전자기 누출 공격(electromagnetic emission attack) 등이 있으며, 특히 장치의 실행에서 전력 소비의 측정과 다른 실행 사이에서 상호 관련성을 찾아 분석하여 공격하는 차분 전력 분석(differential power analysis, DPA) 공격은 가장 강력한 분석법으로 알려져 있다.

[0004] 이러한 차분 전력 분석 공격은 다수의 전력 파형에 대한 신호 처리, 통계적 특성을 이용하여 키를 찾아내는 공

격 방법으로서, 신호 처리 방법에 따라 큰 성능 차이를 가질 수 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명이 해결하고자 하는 기술적 과제는 전력 파형 신호의 특성을 고려하지 않아 전력 분석 공격의 성능이 저하되는 한계를 극복하고, 전력 파형 신호 내에서 전력 분석과 연관된 중요 성분이 신호 압축 과정에서 손실되는 문제점을 해결하는데 있다. 나아가, 본 발명은 전력 파형 신호 내의 다수의 클록에 대해 전력 분석 공격을 위해 신호 압축을 수행함으로 인해 과도한 연산 및 자원이 요구되는 문제점을 해결하고자 한다.

과제의 해결 수단

[0006] 상기 기술적 과제를 해결하기 위하여, 본 발명에 따른 전력 분석 공격을 위한 신호 압축 방법은 전력 파형 신호로부터 적어도 하나 이상의 소정 클록(clock)에 대한 신호를 추출하는 단계; 상기 전력 파형 신호의 특성에 기초하여 상기 추출된 신호의 요소들 각각의 가중치를 결정함으로써 가중치 벡터(weight vector)를 산출하는 단계; 및 상기 추출된 신호의 요소들에 상기 산출된 가중치 벡터를 승산하여 압축 신호를 생성하는 단계를 포함한다.

[0007] 상기 기술적 과제를 해결하기 위하여, 본 발명에 따른 전력 분석 공격을 위한 신호 압축 방법에서 가중치 벡터를 산출하는 단계는 주성분 분석을 이용하여 상기 추출된 신호의 요소들에 대한 압축 신호의 분산이 최대가 되도록 가중치 벡터를 결정하는 것이 바람직하다.

[0008] 상기 또 다른 기술적 과제를 해결하기 위하여, 본 발명에 따른 전력 분석 공격을 위한 신호 압축 방법은 상기 산출된 가중치 벡터를 이용하여 상기 전력 파형 신호의 모든 클록에 대한 압축 신호를 생성하는 단계를 더 포함한다.

[0009] 또한, 이하에서는 상기 기재된 전력 분석 공격을 위한 신호 압축 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

[0010] 상기 기술적 과제를 해결하기 위하여, 본 발명에 따른 전력 분석 공격을 위한 신호 압축 장치는 전력 파형 신호를 입력받는 입력부; 및 상기 입력된 전력 파형 신호로부터 적어도 하나 이상의 소정 클록에 대한 신호를 추출하고, 상기 전력 파형 신호의 특성에 기초하여 상기 추출된 신호의 요소들 각각의 가중치를 결정함으로써 가중치 벡터를 산출하고, 상기 추출된 신호의 요소들에 상기 산출된 가중치 벡터를 승산하여 압축 신호를 생성하는 신호 처리부를 포함한다.

[0011] 상기 기술적 과제를 해결하기 위하여, 본 발명에 따른 전력 분석 공격을 위한 신호 압축 장치에서 상기 가중치 벡터는 주성분 분석을 이용하여 상기 추출된 신호의 요소들에 대한 압축 신호의 분산이 최대가 되도록 하는 값으로 결정되는 것이 바람직하다.

발명의 효과

[0012] 본 발명은 전력 분석 공격을 위한 신호 압축 방법에 있어서 전력 파형 신호의 특성을 고려한 주성분 분석을 이용하여 가중치 벡터를 산출함으로써 전력 분석의 성능을 향상시키고, 전력 파형 신호 내에서 전력 분석과 연관된 중요 성분이 신호 압축 과정에서 온전히 보존되며, 보다 적은 연산 및 자원만으로도 효과적인 전력 분석 결과를 제공할 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법을 도시한 흐름도이다.

도 2는 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법에서 가중치 벡터를 산출하는 과정을 보다 구체적으로 도시한 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법을 설명하기 위해 전력 파형 신호의 한 클록 파형을 예시한 도면이다.

도 4a 내지 4d는 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법에서 산출된 한 클록 신호의 고유 벡터들을 예시한 도면이다.

도 5a 및 도 5b는 각각 전력 파형 신호와 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법에 의해 압축된 신호를 예시한 도면이다.

도 6a 및 도 6b는 본 발명의 또 다른 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법에서 최초에 선택된 하나의 클록 외의 모든 클록들에 대한 압축 신호를 생성하는 방법들을 설명하기 위한 흐름도들이다.

도 7은 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 장치를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 발명의 실시예들을 설명하기에 앞서, 전력 분석 공격을 위한 신호 처리 과정에 대해 개괄적으로 소개하고자 한다.

[0015] 신호 처리 기법은 크게 신호 정렬, 잡음 제거, 신호 압축의 세 단계로 구성된다. 앞서 소개하였던 차분 전력 분석(DPA) 공격에서 신호 압축 기술을 적용했을 때 가장 큰 장점은 분석 수행 시간의 단축과 메모리의 감소이다. 그러나, 신호 압축으로 인해 원래의 전력 파형 신호에서 전력 분석과 연관된 중요한 성분이 손실될 경우, 오히려 분석 성능을 저하시키는 원인이 될 수 있다. 따라서, 고차원의 데이터를 저차원의 데이터로 가공하는 신호 압축을 수행함에 있어, 원래의 전력 파형 신호의 의미 있는 중요 성분이 가능한 손실되지 않도록 할 필요성이 있다. 이러한 신호 압축과 관련하여 Raw integration, Maximum extraction, Sum of squares 등의 방법들이 알려져 있다.

[0016] 이러한 신호 압축 기술은 전력 파형 신호의 특성을 반영하지 않는 다소 직관적인 접근 방법으로부터 도출되었다. 보다 구체적으로 이들 압축 방법을 소개하면 다음과 같다.

[0017] 첫째, Raw Integration 기법은 각 클록(clock) 내의 모든 신호를 더해 하나의 포인트로 압축하는 가장 기본적인 압축 기술이다. 전력 분석의 관점에서 이 기법은 하나의 클록 내의 신호 전부에 모두 동등한 의미를 갖는다. 즉, 하나의 클록 내의 신호들은 모두 동등한 가중치(weight, 중요도를 의미한다.)를 부여받는다.

[0018] 둘째, Maximum Extraction 기법은 각 클록 내의 신호에 대해 최대값을 갖는 하나의 포인트에 대한 신호를 추출하는 압축 기술이다. 이 기법은 하나의 클록 내의 신호에서 가장 많은 전력을 소비하는 위치의 전력을 전력 분석 관점에서 가장 의미있는 신호로 판단하는 방법이다.

[0019] 셋째, Sum of Squares 기법은 각 클록 내의 모든 신호의 제곱 값을 더해 하나의 포인트로 압축하는 기술이다. 이 기법은 이상의 두가지 압축 기술의 특징을 적절히 섞은 것이다. 즉, 하나의 클록 내의 신호에서 가장 많은 전력을 소비하는 위치의 전력을 가장 의미있는 신호로 판단함과 동시에, 소비량이 작은 신호에 대해서도 의미를 부여하는 방법이다. 결국 각 신호 크기만큼 가중치를 주어서 하나의 클록 신호를 더하는 방법이다.

[0020] 그러나, 상기된 세 가지 압축 기법들은 상당히 직관적인 방법으로 신호의 특성을 전혀 고려하지 않았기 때문에 차분 전력 분석(DPA)의 성능을 저하시키는 원인이 될 수 있다. 특히, 상기된 압축 기법들은 신호의 특성에 따라 가중치를 각각의 신호 요소들에 대해 차별적이고 개별적으로 부여되지 않는다는 점에서 한계를 가진다.

[0021] 구체적으로, 전력 분석을 위한 신호 압축 기술에서 하나의 클록 내의 신호는 다음의 수학식 1과 같이 m 개의 신호 요소들(신호의 포인트들을 의미한다.)의 집합으로 표현될 수 있다.

수학식 1

[0022] $$x = [x(1), x(2), ..., x(m)]$$

[0023] 또한, 이러한 신호 x의 각각의 요소들에 대한 최적의 가중치 벡터(weight vector)는 다음의 수학식 2와 같이 표현될 수 있다.

수학식 2

$$w = [w(1), w(2), ..., w(m)] \; (\parallel w \parallel = \sqrt{\sum_{t=1}^{m} w(t)^2} = 1)$$

[0024]

[0025] 여기서 최적의 가중치 벡터란, 해당 신호를 최적으로 압축시키기 위한 각각의 신호 요소들에 대한 가중치들을 의미한다. 따라서, 어떠한 압축 신호 또는 어떠한 가중치 벡터가 최적이 되느냐의 문제는 결국 해당 신호의 특성을 정확하게 파악하고 반영할 수 있는지의 문제로 귀결된다. 다시 말해, 원래의 신호의 특성을 정확하게 파악하지 못한다면 최적의 압축 신호를 생성한다는 것은 매우 어려운 일이 될 것이다. 따라서, 전력 분석을 위한 최적의 신호 압축 기술은 하나의 클록 내의 신호 x의 각 신호 요소들에 대해 전력 파형 신호의 특성을 고려한 최적의 가중치 벡터 ω를 찾는 것을 의미한다.

[0026] 이렇게 발견된 가중치 벡터에 의해 원래의 전력 파형 신호 벡터는 다음의 수학식 3과 같이 하나의 포인트 신호로 압축될 수 있다.

수학식 3

$$S = w^T x = \sum_{t=1}^{m} w(t)x(t)$$

[0027]

[0028] 수학식 3은 전력 파형 신호의 m 개의 요소들에 대응하는 m 개의 가중치 벡터를 각각 승산한 후에, 승산한 결과들을 모두 가산하여 하나의 신호로 압축하였음을 나타낸다.

[0029] 이제 앞서 소개한 바 있는 세 가지 신호 압축 기술에서 가중치 벡터가 어떠한 방식으로 적용되었는지를 검토하기 위해 다음의 표 1을 참조하자. 이들 세 가지 신호 압축 기술 역시 가중치 벡터를 활용하여 신호를 압축하게 되는데, 각각의 신호 압축 기술들은 서로 상이한 가중치 벡터를 활용한다.

표 1

신호 압축 기법	weight vector $w = [w(1), w(2), ..., w(m)]$ (원신호 $x = [x(1), x(2), ..., x(m)]$)
Raw integration	$w = [\frac{1}{\sqrt{m}}, \frac{1}{\sqrt{m}}, ..., \frac{1}{\sqrt{m}}]$
Maximum Extraction	$\begin{cases} w(t) = 1 & ; x(t) \; is \; maximum \; in \; \{x(1), x(2), ..., x(m)\} \\ w(t) = 0 & ; otherwise \end{cases}$
Sum of Squares	$w(t) = \frac{x(t)}{\parallel x \parallel}$

[0030]

[0031] 이상의 표 1에서 확인할 수 있듯이 앞서 소개된 세 가지 신호 압축 기술들은 매우 직관적이기는 하나, 각각의 신호 요소들의 특성을 전혀 고려하고 있지 못하며, 심지어 일부 기술들에서는 신호들간의 중요도의 차이가 전혀 반영되어 있지 않다. 따라서, 원래의 신호의 특성이 신호 압축 기술에 적용되지 않았으므로, 결과적으로 최적의 압축 신호를 생성하는데 근본적인 한계점을 갖는다.

[0032] 이하에서는 본 발명의 다양한 실시예들을 통해 상기된 신호 압축 기술들의 한계를 극복할 수 있는 신호 압축 기술을 제안하고자 한다. 본 발명의 실시예들을 통해 소개될 신호 압축 기술은 주성분 분석(principal component

analysis, PCA)을 이용한 것으로, 전력 파형 신호의 특성을 고려한 신호 압축 기술에 해당한다.

[0033] 통계학에서 주성분 분석이란 데이터 집합을 분석하는 기법 가운데 하나로서, 데이터를 한 개의 축으로 사상시켰을 때, 그 분산이 가장 커지는 축이 첫 번째 좌표축으로 위치하고, 두 번째로 커지는 축이 두 번째 좌표축으로 위치하게 되는 식으로, 순차적으로 데이터를 좌표계로 선형 변환하는 기법을 말한다. 이와 같이 각각의 축에 데이터의 가장 중요한 성분을 위치시킴으로써, 주성분 분석은 가장 큰 분산을 갖는 부공간(subspace)을 보존하는 최적의 선형 변환이라는 특징을 나타낸다. 특히, 주성분 분석은 통상적인 선형 변환과는 달리 정해진 가중치 벡터를 갖지 않으며, 주어진 데이터의 특성에 따라 결정될 수 있다는 장점을 갖는다. 따라서, 앞서 설명한 바와 같이 전력 분석을 위한 신호 압축 기술에서 신호의 특성을 고려한 최적의 가중치 벡터를 찾는 데에 적절하게 이용될 수 있다. 즉, 본 발명의 실시예들에서 주성분 분석은 원신호에서 전력 분석에 의미가 있는 신호를 데이터 값에 의존해 변동이 큰 신호 값으로 판단하는데 활용된다.

[0034] 이하에서, 도면을 참조하여 본 발명의 다양한 실시예들을 상세하게 설명한다.

[0035] 도 1은 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법을 도시한 흐름도로서, 다음과 같은 단계들을 포함한다.

[0036] 110 단계에서 전력 파형 신호로부터 적어도 하나 이상의 소정 클록에 대한 신호를 추출한다. 여기서 소정 클록(predetermined clock)이란 다수의 클록들 중에서 선택된 하나의 클록이 될 수 있다. 만약 다수의 클록에서 소비된 전력을 한 번에 주성분 벡터를 이용해 변환한다는 신호 고유의 선형성을 잃어버릴 수 있기 때문에 신호 압축은 하나의 클록에 대한 연산 상에서 이루어지는 것이 보다 효과적일 수 있다. 즉, 110 단계는 전력 파형 신호 중 하나의 클록을 선택하여 해당 클록에 대한 신호를 추출한다.

[0037] 특히, 소프트웨어로 구현된 암호 연산기는 다수의 클록 동안 동작하므로 매 클록마다 유사한 전력 분석을 반복 수행할 경우 지나치게 많은 연산을 수행하게 되고, 그 결과 과도한 컴퓨팅 파워(computing power) 및 자원(resource)를 소모하게 된다. 따라서, 이러한 경우 경제성 측면에서 특정 클록에 대해서만 가중치 벡터를 산출한 후, 나머지 클록들에 산출된 가중치 벡터를 활용하여 신호 압축을 수행할 수도 있을 것이다.

[0038] 한편, 원래의 전력 파형 신호가 입력된 경우 상기된 신호 추출 단계는 전자적 형태로 수신된 신호 정보를 처리하는 과정에 해당하므로, 신호 추출을 수행할 수 있는 처리기(processor) 및 이러한 연산에 필요한 기억공간(memory)을 통해 구현될 수 있을 것이다. 또한, 이러한 처리기 및 기억공간은 본 발명이 속하는 기술분야의 활용 환경이나 동작 환경을 고려하여 통상의 기술자에 의해 적절하게 선택될 수 있을 것이다. 나아가, 이러한 신호 추출 단계는 이상에 예시된 하드웨어뿐만 아니라 이상의 신호 추출 과정에 활용되거나 예시된 하드웨어들을 제어할 수 있는 부가적인 소프트웨어 코드(code)에 의해서도 구현될 수 있다.

[0039] 120 단계에서는 전력 파형 신호의 특성에 기초하여 110 단계에서 추출된 신호의 요소들 각각의 가중치를 결정함으로써 가중치 벡터를 산출한다. 120 단계는 앞서 소개한 세 가지 신호 압축 기술들과는 달리 전력 파형 신호의 특성을 고려함으로써 최적의 가중치 벡터를 산출할 수 있으며, 각각의 신호 요소들에 대해 동일한 가중치가 아닌 개별적인 가중치를 부여하게 된다.

[0040] 특히, 120 단계에서 가중치 벡터를 산출하는 과정은 주성분 분석을 이용하여 110 단계를 통해 추출된 신호의 요소들에 대한 압축 신호의 분산이 최대가 되도록 가중치 벡터를 결정한다. 따라서, 앞서 언급한 바와 같이 신호의 요소들 각각에 대응하는 가중치 벡터가 미리 결정되거나 고정된 값이 아니며, 신호의 특성을 고려하여 개별적으로 결정되는 값에 해당한다.

[0041] 최적의 가중치 벡터를 찾기 위해 주성분 분석의 개념을 활용하는 과정은 다음과 같다. 전력 분석 공격에 이용되는 n 개의 클록 신호는 다음과 같이 수학식 4와 같이 표현될 수 있다. 여기서 각각의 클록 신호의 하나의 클록에 해당하는 신호를 나타낸다.

수학식 4

[0042] $$x_i = [x_i(1), x_i(2), ..., x_i(m)](1 \le i \le n)$$

[0043] 본 발명의 실시예에서 최적의 가중치 벡터를 찾는 것은 상기된 n 개의 클록 신호에 대해 다음의 수학식 5를 만

족하는 가중치 벡터 $g=[g(1),g(2),...,g(m)]$ 를 찾는 것을 의미한다.

수학식 5

[0044] $$g=\mathrm{argmax}_w\ Var\{w^Tx_1,w^Tx_2,...,w^Tx_n\}$$

[0045] 수학식 5에서 argmax는 압축 신호의 분산을 최대로 만드는 가중치 벡터를 의미한다. 이러한 가중치 벡터를 찾는 작업은 원래의 전력 파형 신호에서 전력 분석에 의미가 있는 신호를 데이터 값에 의존해 변동이 큰 신호 값으로 판단하는 주성분 분석에 근거하여 수행된다. 즉, 최적의 가중치 벡터를 산출하는 단계는 전력 파형 신호의 변동이 큰 신호에 상대적으로 더 큰 가중치를 부여하는 것을 의미한다. 따라서, 주성분 분석에 의해 ω 값을 찾게 되면, 상기 수학식 5에 의해 g 값이 결정될 수 있게 된다. 압축 신호의 분산이 최대가 되도록 가중치 벡터를 결정하는 보다 구체적인 방법과 원리는 도 2를 통해 후술하도록 하겠다.

[0046] 이러한 가중치 벡터의 산출 단계는 전자적 형태로 가공된 전력 파형 신호로부터 추출된 신호의 요소들로부터 가중치 벡터를 산출하는 과정에 해당하므로, 상기된 연산을 수행할 수 있는 처리기 및 기억공간이 앞서 설명한 110 단계와 유사한 방법으로 활용될 수 있다. 또한, 이러한 처리기 및 기억공간을 제어하기 위한 부가적인 소프트웨어 코드가 활용될 수 있음은 당연하다.

[0047] 130 단계에서는 110 단계를 통해 추출된 신호의 요소들에 120 단계를 통해 산출된 가중치 벡터를 승산하여 압축 신호를 생성한다. 앞서 수학식 3을 통해 설명한 바와 같이 원래의 전력 파형 신호의 각 요소들에 120 단계를 통해 산출된 가중치 벡터를 승산한 후, 승산 결과값을 모두 가산함으로써 하나의 압축 신호를 생성할 수 있다. 이 때의 압축 신호는 앞서 120 단계를 통해 전력 파형 신호의 특성을 고려하여 산출된 최적화된 가중치 벡터에 의한 결과이므로 신호 요소들 중의 중요한 요소가 소실되지 않은 압축 신호에 해당한다.

[0048] 이러한 압축 신호를 생성하는 과정은 전자적 형태로 가공된 신호 요소들과 전자적 형태로 가공된 가중치 벡터를 활용하여 최종 산출물인 압축 신호를 생성하는 과정에 해당하므로, 이들 연산을 수행할 수 있는 처리기 및 기억공간이 활용될 수 있다. 또한, 이러한 처리기 및 기억공간을 제어하기 위한 부가적인 소프트웨어 코드가 활용될 수 있음은 당연하다.

[0049] 상기된 본 발명의 실시예에 따르면 전력 분석 공격을 위한 신호 압축 방법에 있어서 전력 파형 신호의 특성을 고려한 주성분 분석을 이용하여 가중치 벡터를 산출함으로써 전력 분석의 성능을 향상시키고, 전력 파형 신호 내에서 전력 분석과 연관된 중요 성분이 신호 압축 과정에서 온전히 보존되며, 보다 적은 연산 및 자원만으로도 효과적인 전력 분석을 수행하는 것이 가능하다.

[0050] 도 2는 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법에서 가중치 벡터를 산출하는 과정(도 1의 120 단계)을 보다 구체적으로 도시한 흐름도로서, 도 1의 110 단계와 130 단계는 편의상 생략되었다. 즉, 도 2에서는 추출된 신호가 입력되는 과정부터 기술하도록 하겠다. 이 때의 입력 신호는 n 개의 전력 파형 신호 각각에 대해 하나의 클록에 해당하는 신호를 추출한 것이다. 또한, 이하에서 변수 m은 클록 사이즈를 의미하고, 변수 p는 선택한 주성분 수를 의미한다.

[0051] 전력 분석 공격을 수행하기 위해서는 신호 압축을 수행하더라도 데이터 값의 해밍 웨이트(Hamming weight) 또는 해밍 디스턴스(Hamming distance)에 의존한 전력 소비 패턴이 유지되어야 한다. 앞서 언급한 바와 같이 만약 다수의 클록에서 소비된 전력을 한 번에 주성분 벡터를 이용해 변환한다면 이러한 선형성을 잃어버릴 수 있게 된다. 따라서, 본 발명의 실시예들에서 신호 압축은 하나의 클록의 연산 상에서 이루어져야만 한다.

[0052] 121 단계에서 추출된 신호의 요소들로부터 공분산 행렬(covariance matrix)을 산출한다. 추출된 신호들을 $X=\{x_1,x_2,....,x_n\}$ 라 할 때, 추출된 신호들에 대한 압축 신호들로 이루어진 분포 $Z=Var\{w^Tx_1,w^Tx_2,...,w^Tx_n\}$ 에 대해 Var(Z)의 값은

[0053] 다음의 수학식 6과 같이 변형될 수 있다.

수학식 6

$$Var(Z) = \frac{1}{n}\sum_{i=1}^{n}(w^T x_i - w^T \overline{x})^2 = \frac{1}{n}\sum_{i=1}^{n} w^T (x_i - \overline{x})(x_i - \overline{x})^T w = w^T S w$$

[0054]

[0055] 여기서, 공분산 행렬(covariance matrix)과 평균 벡터(mean vector)는 다음의 수학식 7과 같이 정리된다.

수학식 7

$$S(covariance\ matrix) = \frac{1}{n}\sum_{i=1}^{n}(x_i - \overline{x})(x_i - \overline{x})^T$$

[0056]

$$\overline{x}(mean\ vector) = \frac{1}{n}\sum_{i=1}^{n} x_i$$

[0057]

[0058] 122 단계에서는 121 단계를 통해 산출된 공분산 행렬로부터 고유 벡터들과 고유 값들을 산출한다. 앞서 검토한 수학식 7에서 Var(Z)가 최대값을 갖도록 하는 벡터 ω를 찾는 작업은 다음의 수학식 8과 같이 수행된다.

수학식 8

$$Var(Z) = w^T S w - \lambda(w^T w - 1)$$

$$\frac{\partial Var(Z)}{\partial w} = 2Sw - 2\lambda w = 0$$

$$\Rightarrow \qquad Sw = \lambda w \qquad \text{a}$$

$$\Rightarrow \qquad Var(Z) = w^T S w = \lambda \qquad \text{s}$$

[0059]

[0060] 수학식 8에서 Var(Z)를 ω로 편미분하여 0 이 되도록 하는 벡터 ω는 Var(Z)가 최대가 되도록 하는 후보 벡터가 될 수 있다. 이러한 작업은 데이터 벡터들의 공분산 행렬의 고유 벡터와 고유 값을 찾는 문제로 귀결된다.

[0061] 위의 수학식 8에서 보는 바와 같이 해당 고유 벡터들에 대하여 선형 변환을 수행했을 때의 분산 값은 대응되는 고유 값이 된다. 따라서 가장 큰 고유 값을 갖는 고유 벡터가 수학식 5를 만족하는 g가 된다.

[0062] 123 단계에서는 122 단계를 통해 산출된 고유 값들 중 상대적으로 값이 큰 고유 값들에 대응하는 소정 개수의 고유 벡터들을 선택한다.

[0063] 여기서 소정 개수(predetermined number)의 고유 벡터를 선택한다 함은 원래의 전력 파형 신호와 유사한 신호를 남기고 유사하지 않은 신호를 제거하기 위함이다. 이 때, 고유 벡터를 선택하는 개수는 사용자의 필요에 따라 자유롭게 설정될 수 있다. 따라서, 122 단계를 통해 산출된 고유 값들 중에서 값이 큰 것들을 특정 개수만큼 선택할 경우, 이렇게 선택된 고유 값들에 대응하는 특정 개수의 고유 벡터들이 선택될 것이다.

[0064] 앞서 정리한 수학식 8에서 $Sw = \lambda w$ 를 만족하는 고유 벡터 ω는 S의 rank 만큼 존재하게 되며, 각 고유 벡터들은 서로 직교하는 성질을 갖는다. 따라서, 찾고자 하는 선형 변환 벡터는 고유 값 λ중 큰 값 순서대로 고유 벡터를 선택해 사용할 수 있다. 만약, $\lambda_1 \geq \lambda_2 \geq .... \geq \lambda_k$ 의 순서대로 고유 값들이 정렬되고, 각각의 고유 값 λ_i 에 해당하는 고유 벡터를 ω_i라고 한다면, 고유 값이 큰 p개의 고유 벡터들 (ω_1, ω_2, ..., ω_p)을 주성분 벡터로 투영해서 사용할 벡터들로 선택하면 된다.

[0065] 한편, 이상에서 고유 벡터를 선택하는 단계는 전력 파형 신호와 상관도가 낮은 고유 벡터를 일정 개수만큼 소거함으로써 수행될 수 있다. 즉, 시각적으로 원신호와 연관도가 떨어지는 고유 벡터를 잡음 성분으로 판단하여 소거한다. 이해를 돕기 위해 이러한 과정을 도 3, 도 4a 내지 도 4d를 참조하여 설명하면 다음과 같다.

[0066] 도 3은 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법을 설명하기 위해 전력 파형 신호의 한 클록 파형을 예시한 도면이며, 도 4a 내지 4d는 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법에서 산출된 한 클록 신호의 고유 벡터들을 예시한 도면이다.

[0067] 우선 도 3에 예시된 신호의 파형을 주시하자. 다음으로, 도 3의 전력 파형 신호에 기초하여 생성된 도 4a 내지 도 4d의 4 개의 고유 벡터를 살펴보자. 4 개의 고유 벡터 파형 중, 도 4a 및 도 4b는 상대적으로 도 3의 원래의 전력 파형 신호와 그 패턴이 유사하다. 즉, 시각적으로 원신호와 연관도가 높다. 반면, 도 4c 및 도 4d는 상대적으로 도 3의 원래의 전력 파형 신호와 시각적으로 연관도가 떨어진다. 따라서, 소정 개수를 2개라고 설정하였다면, 도 4a 및 도 4b의 2개의 고유 벡터만을 선택하고 나머지 고유 벡터들을 소거한다.

[0068] 이러한 시각적으로 연관도가 높은 고유 벡터를 선택하는 과정은 산출된 고유 벡터 그래프의 패턴을 비교하거나, 원신호와 고유 벡터 패턴과의 상관도를 산출함으로써 수행될 수 있는데, 이를 위해 그래프의 패턴을 비교하는 다양한 비교 수단이 활용될 수 있다. 이러한 그래프의 시각적인 연관도를 산출하는 비교 수단은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 본 실시예가 적용되는 구현 환경에 따라 적절하게 선택될 수 있다.

[0069] 다시 도 2로 돌아와, 124 단계에서는 123 단계를 통해 선택된 고유 벡터들을 가산하여 가중치 벡터를 산출한다. 앞서 설명한 실시예에 따를 경우 123 단계에서 선택된 p개의 고유 벡터들을 가산함으로써 가중치 벡터를를 산출할 수 있다.

[0070] 이상에서 가중치 벡터를 산출하는 구체적인 과정을 설명하였다. 이미 도 1의 120 단계를 통해 소개한 바와 같이 이상의 구체적인 연산들을 수행할 수 있는 처리기, 기억공간 및 이러한 하드웨어들을 제어하기 위한 부가적인 소프트웨어 코드가 활용될 수 있음은 당연하다.

[0071] 도 5a 및 도 5b는 각각 전력 파형 신호와 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법에 의해 압축된 신호를 예시한 도면으로, 특히 도 5b는 산출된 가중치 벡터를 활용하여 전력 파형 신호의 각각의 신호 요소들을 압축함으로써 생성된 압축 신호를 도시하였다.

[0072] 도 2를 통해 열거된 과정에 의해 가중치 벡터가 산출된 이후에, 산출된 가중치 벡터를 이용하여 원래의 전력 파형 신호의 n개의 클록 신호들을 각각 하나의 포인트로 압축할 수 있다. 이러한 압축에는 앞서 설명한 수학식 3이 활용된다. 도시된 도 5b의 그래프는 본 발명의 실시예를 통해 제안하고 있는 가중치 벡터에 암호 알고리즘으로 널리 알려진 DES 알고리즘을 활용하여 생성된 것이다.

[0073] 도 5a 및 도 5b에서 보는 바와 같이 양의 방향으로만 소비되던 신호가 신호 압축 후, 양과 음의 방향으로 분포됨을 확인할 수 있다. 이는 각 클록 신호에 대해 주성분 분석을 수행했을 때, 고유 벡터의 성분은 동일하나 방향이 반대가 될 수 있기 때문에 나타나는 현상이다. 그러나, 이러한 현상은 전력 분석을 수행했을 때, 상관 계수의 절대값을 비교하면 되므로 문제가 되지 않는다.

[0074] 이상에서 제시된 본 발명의 실시예들은 하나의 클록에 대한 압축 신호를 생성하는 방법들을 소개하였다. 이제 이러한 하나의 클록뿐만 아니라 전력 분석 공격을 위한 대상 신호 내에 포함된 모든 클록들에 대한 압축 신호를 생성하는 2 가지 실시예를 제시하고자 한다.

[0075] 도 6a 및 도 6b는 본 발명의 또 다른 실시예에 따른 전력 분석 공격을 위한 신호 압축 방법에서 최초에 선택된 하나의 클록 외의 모든 클록들에 대한 압축 신호를 생성하는 방법들을 설명하기 위한 흐름도들이다. 각 흐름도

에서 110 단계 내지 130 단계는 이미 도 1을 통해 설명한 바 있으므로 여기서는 자세한 설명을 생략한다.

[0076] 도 6a는 도 1의 전력 분석 공격을 위한 신호 압축 방법에서 140 단계를 추가적으로 포함한다. 140 단계는 120 단계 및 130 단계를 통해 전력 파형 신호로부터 하나의 클록에 대한 가중치 벡터를 산출하고 이에 대한 압축 신호를 생성하는 과정을 전력 파형 신호의 클록들 각각에 대해 반복적으로 수행한다. 이러한 과정을 통해 동일한 클록 사이즈를 갖는 여타의 모든 클록들을 포함하는 전력 파형 신호에 대해서도 최적화된 압축 신호를 생성할 수 있다.

[0077] 그러나, 소프트웨어로 구현된 암호 연산기는 다수의 클록 동안 반복적으로 수행되므로, 매 클록마다 상기 열거된 가중치 벡터의 산출 과정 및 압축 신호의 생성 과정을 반복하여 수행하는 것은 많은 연산량과 컴퓨팅 파워, 자원 소모를 요구한다. 따라서, 이러한 경우 특정 클록에 대해서만 가중치 벡터를 산출한 후, 나머지 모든 클록에 산출된 가중치 벡터를 적용할 수도 있다. 이하에서 도 6b를 통해 이러한 실시예를 검토한다.

[0078] 도 6b는 도 1의 전력 분석 공격을 위한 신호 압축 방법에서 150 단계를 추가적으로 포함한다. 150 단계에서는 130 단계를 통해 산출된 가중치 벡터를 이용하여 전력 파형 신호의 모든 클록에 대한 압축 신호를 생성한다. 즉, 가중치 벡터 산출을 위해 선택된 하나의 클록뿐만 아니라 전력 분석 공격을 위한 대상 신호 내의 모든 클록에 대해 앞서 산출된 가중치 벡터를 적용한다.

[0079] 이러한 본 발명의 실시예에 따르면, 전력 파형 신호 내에서 전력 분석과 연관된 중요 성분이 신호 압축 과정에서 온전히 보존되면서, 보다 적은 연산 및 자원만으로도 효과적인 전력 분석 결과를 제공할 수 있다.

[0080] 도 7은 본 발명의 일 실시예에 따른 전력 분석 공격을 위한 신호 압축 장치(700)를 도시한 도면으로, 이미 설명한 도 1의 실시예를 장치를 통해 구현한 실시예에 해당한다. 도 7의 신호 압축 장치(700)는 크게 입력부(710)와 신호 처리부(720)를 포함하며, 신호 처리부(720)는 보다 구체적으로 신호 추출부(721), 가중치 벡터 산출부(722) 및 압축 신호 생성부(723)을 포함한다.

[0081] 입력부(710)는 원신호인 전력 파형 신호를 입력받는다. 이 때, 전력 파형 신호는 아날로그 형태의 데이터가 수신될 수도 있고, 디지털 형태로 가공된 데이터가 수신될 수도 있다. 만약 전력 파형 신호가 아날로그 형태로 입력될 경우, 신호 처리의 편의를 위해 이를 디지털 형태의 신호로 가공하는 구성(ADC)이 수반될 수 있을 것이다.

[0082] 신호 처리부(720)에서, 보다 구체적으로 신호 추출부(721)는 입력부(710)를 통해 입력된 전력 파형 신호로부터 소정 클록에 대한 신호를 추출한다. 이러한 구성은 앞서 도 1의 110 단계에 대응하는 것으로 구체적인 설명은 생략한다.

[0083] 다음으로 가중치 벡터 산출부(722)는 전력 파형 신호의 특성에 기초하여 신호 추출부(721)를 통해 추출된 신호의 요소들 각각의 가중치를 결정함으로써 가중치 벡터를 산출한다. 또한, 가중치 벡터는 주성분 분석을 이용하여 신호 추출부(721)를 통해 추출된 신호의 요소들에 대한 압축 신호의 분산이 최대가 되도록 하는 값으로 결정될 수 있다. 나아가, 보다 구체적으로 가중치 벡터 산출부(722)는 신호 추출부(721)를 통해 추출된 신호의 요소들로부터 공분산 행렬을 산출하고, 산출된 공분산 행렬로부터 고유 벡터들과 고유 값들을 산출하고, 산출된 고유 값들 중 값이 큰 고유 값들에 대응하는 소정 개수의 고유 벡터들을 선택하고, 선택된 고유 벡터들을 가산함으로써 가중치 벡터를 산출할 수 있다. 이러한 구성은 앞서 도 1의 120 단계에 대응하는 것으로 구체적인 설명은 생략한다.

[0084] 이어서 압축 신호 생성부(723)는 신호 추출부(721)를 통해 추출된 신호의 요소들에 가중치 벡터 산출부(722)를 통해 산출된 가중치 벡터를 승산하여 압축 신호를 생성한다. 이러한 구성은 앞서 도 1의 130 단계에 대응하는 것으로 구체적인 설명은 생략한다.

[0085] 이상에서 기술한 신호 처리부(720)의 요소들은 상기된 일련의 연산을 수행할 수 있는 처리기 및 기억공간이 활용될 수 있다. 또한, 이러한 처리기 및 기억공간을 제어하기 위한 부가적인 소프트웨어 코드가 활용될 수 있음은 당연하다.

[0086] 상기된 본 발명의 실시예에 따르면 전력 분석 공격을 위한 신호 압축 장치에 있어서 전력 파형 신호의 특성을 고려한 주성분 분석을 이용하여 가중치 벡터를 산출함으로써 전력 분석의 성능을 향상시키고, 전력 파형 신호 내에서 전력 분석과 연관된 중요 성분이 신호 압축 과정에서 온전히 보존되며, 보다 적은 연산 및 자원만으로도 효과적인 전력 분석을 수행하는 것이 가능하다.

[0087] 한편, 본 발명은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기

록 장치를 포함한다.

[0088] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[0089] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0090] 700 : 전력 분석 공격을 위한 신호 압축 장치

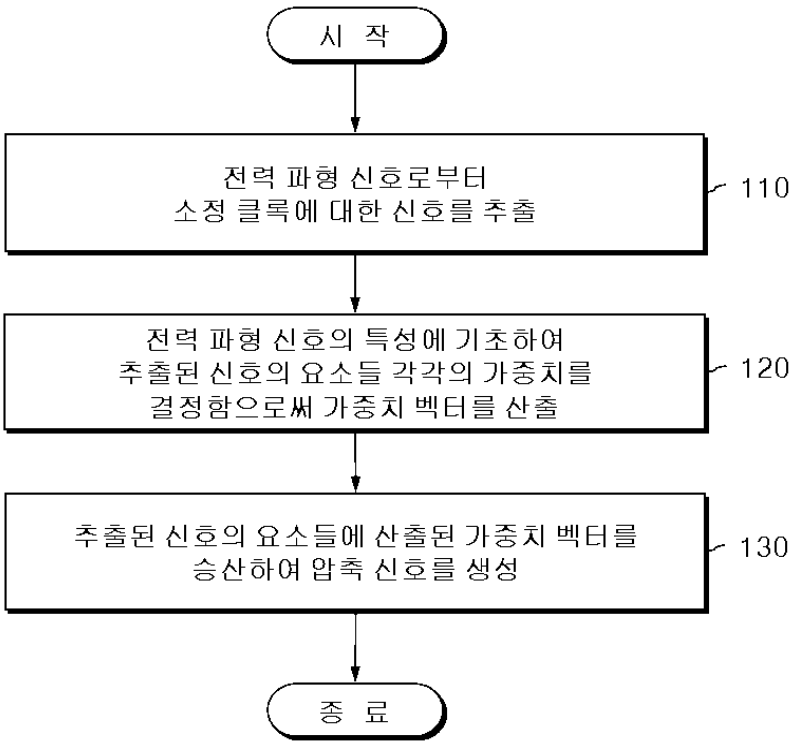
710 : 입력부

720 : 신호 처리부 721 : 신호 추출부

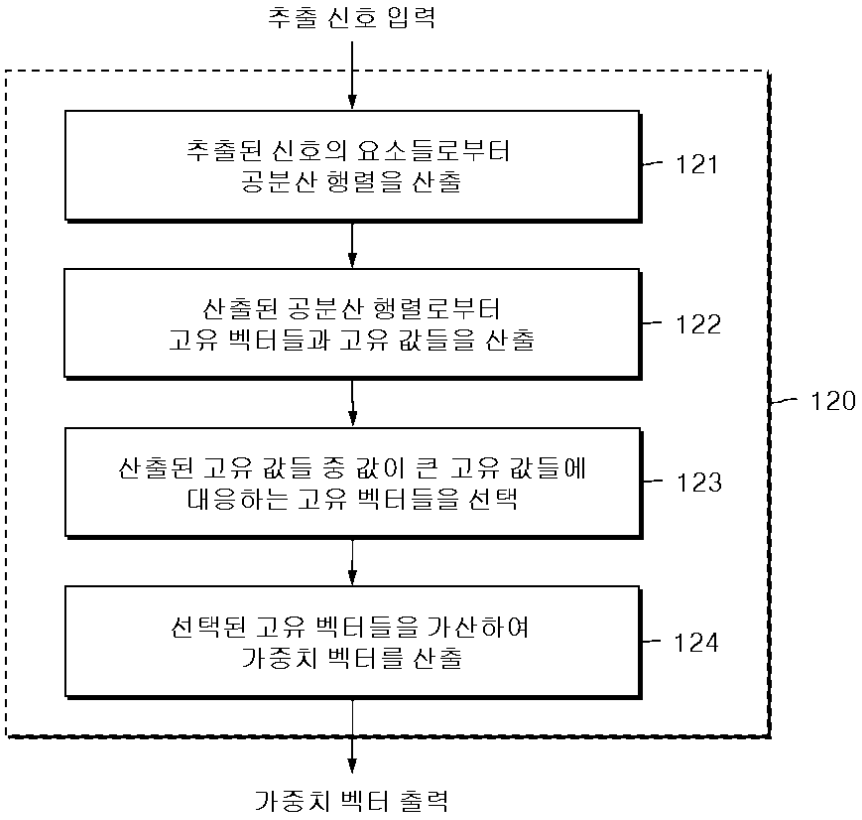
722 : 가중치 벡터 산출부 723 : 압축 신호 생성부

도면

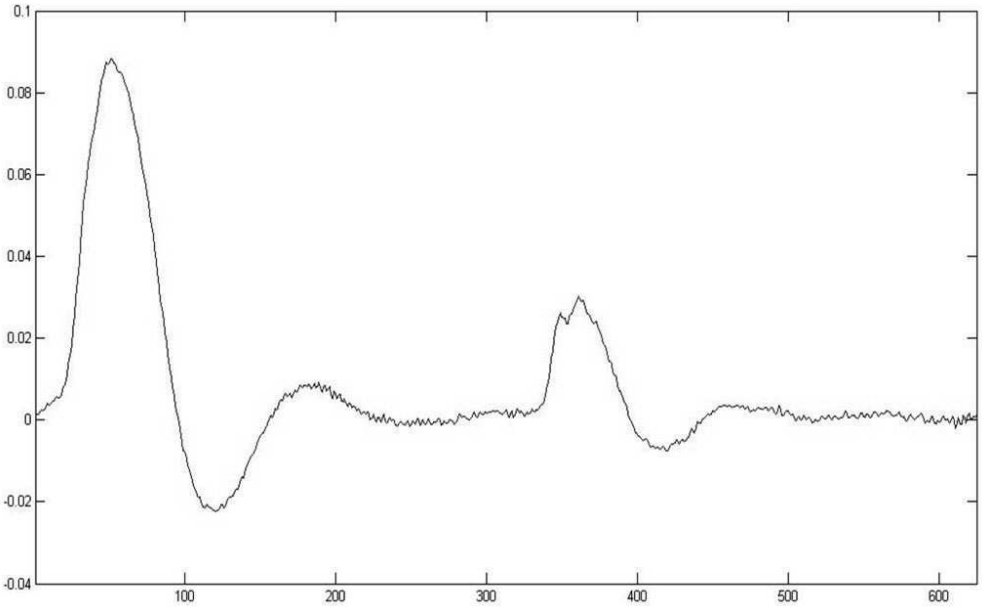
도면1



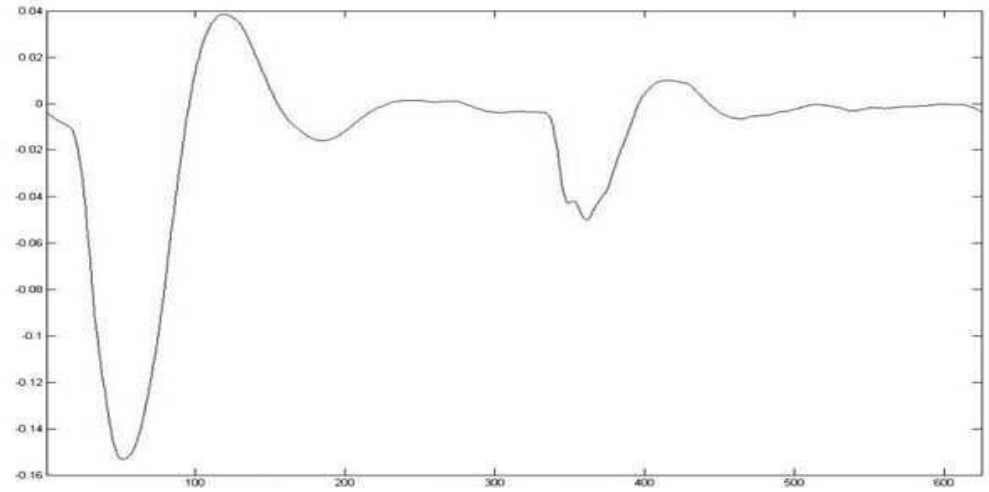
도면2


추출 신호 입력
추출된 신호의 요소들로부터
공분산 행렬을 산출
121
산출된 공분산 행렬로부터
고유 벡터들과 고유 값들을 산출
122
120
산출된 고유 값들 중 값이 큰 고유 값들에
대응하는 고유 벡터들을 선택
123
선택된 고유 벡터들을 가산하여
가중치 벡터를 산출
124
가중치 벡터 출력

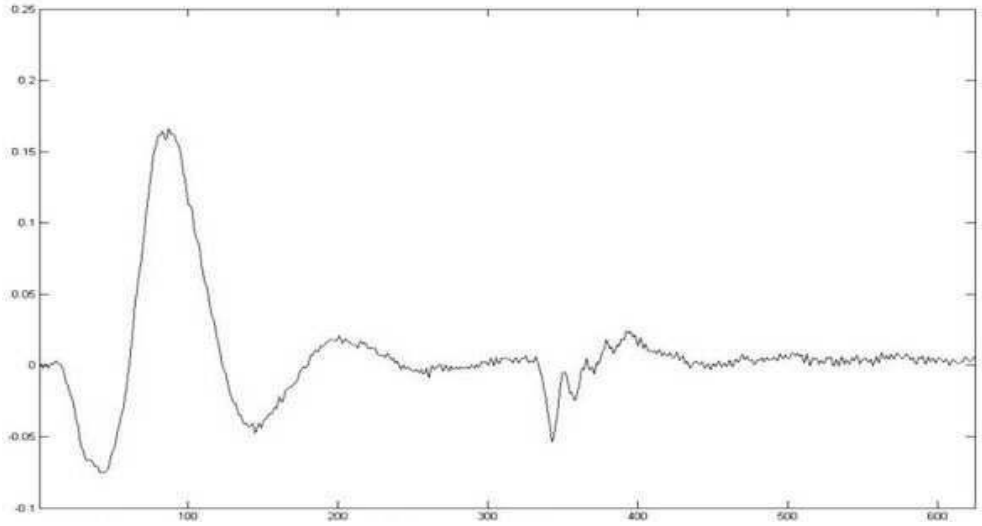
도면3


0.1
0.08
0.06
0.04
0.02
0
-0.02
-0.04
100
200
300
400
500
600

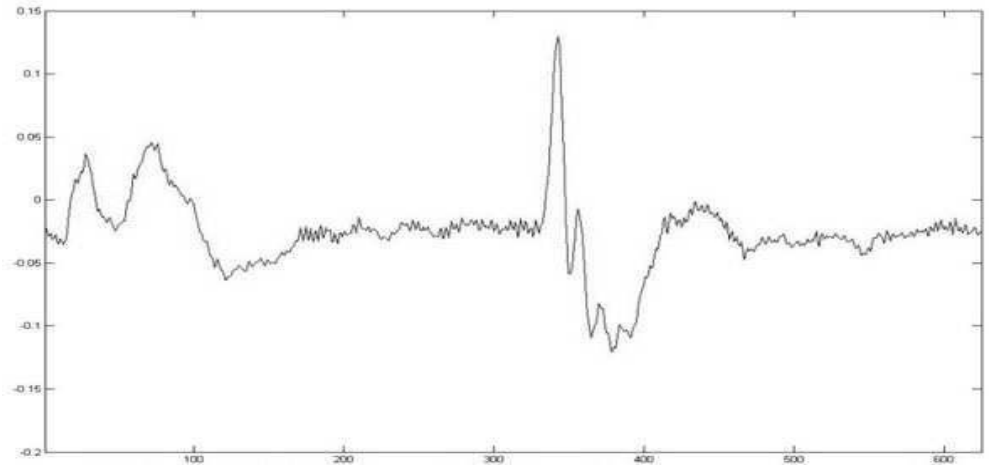
도면4a



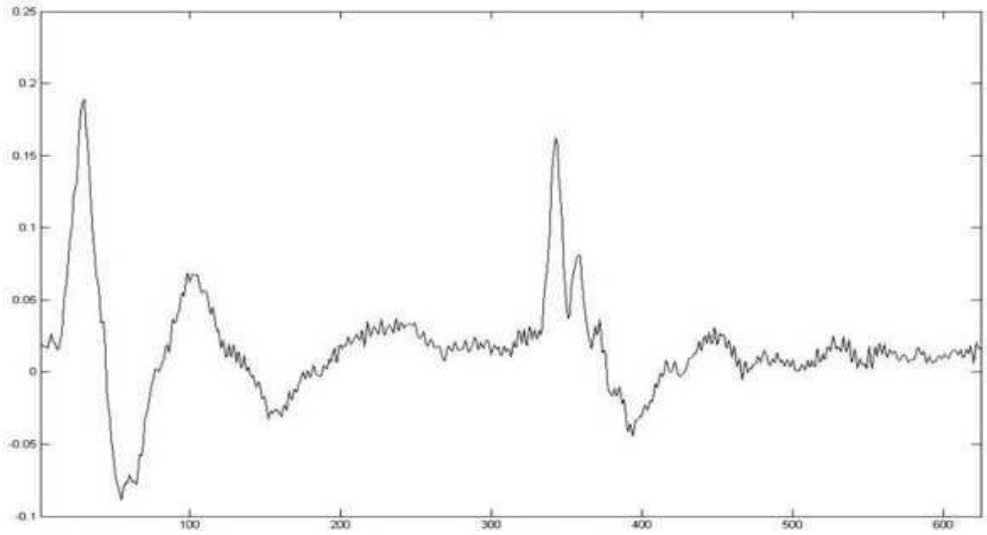
도면4b



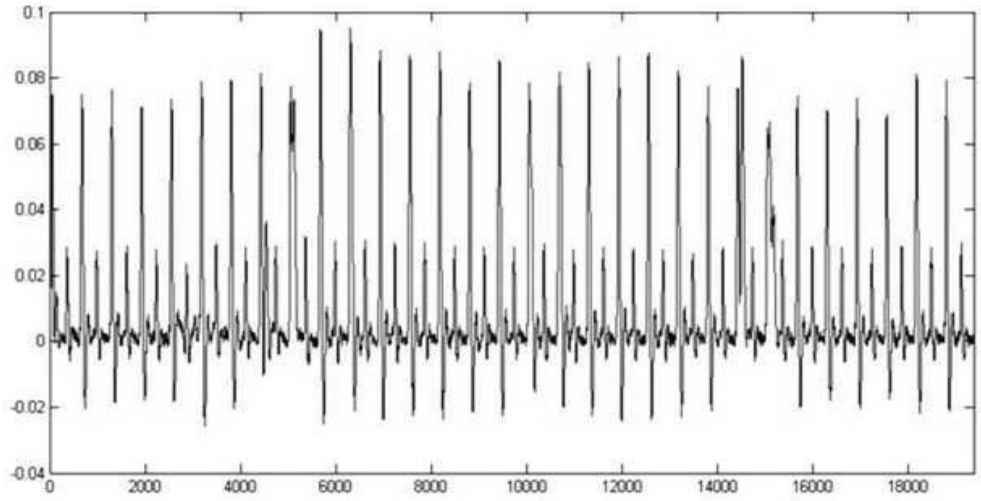
도면4c



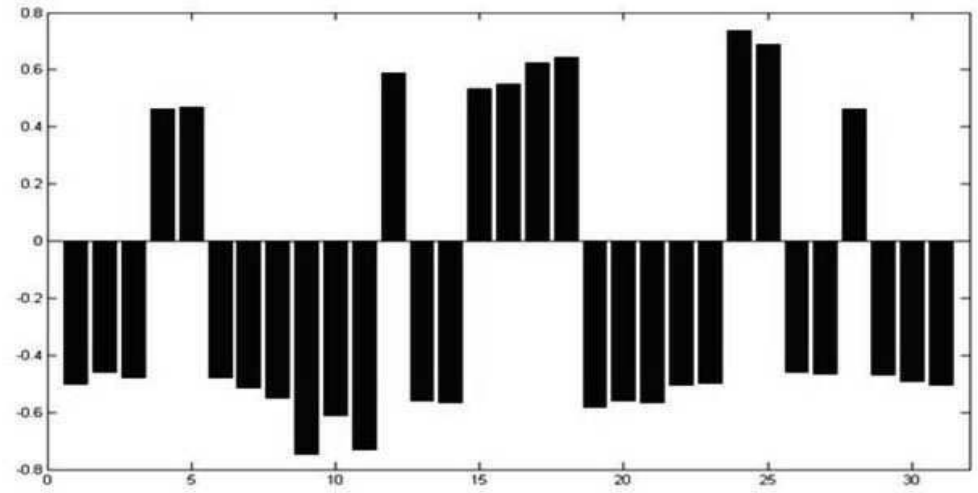
도면4d



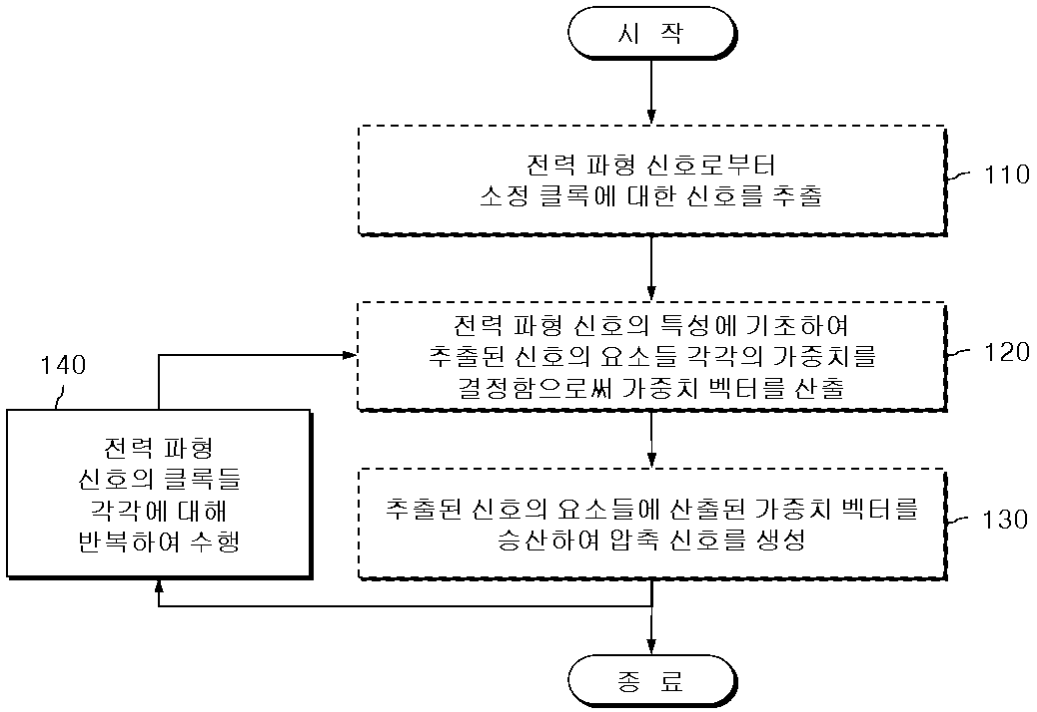
도면5a



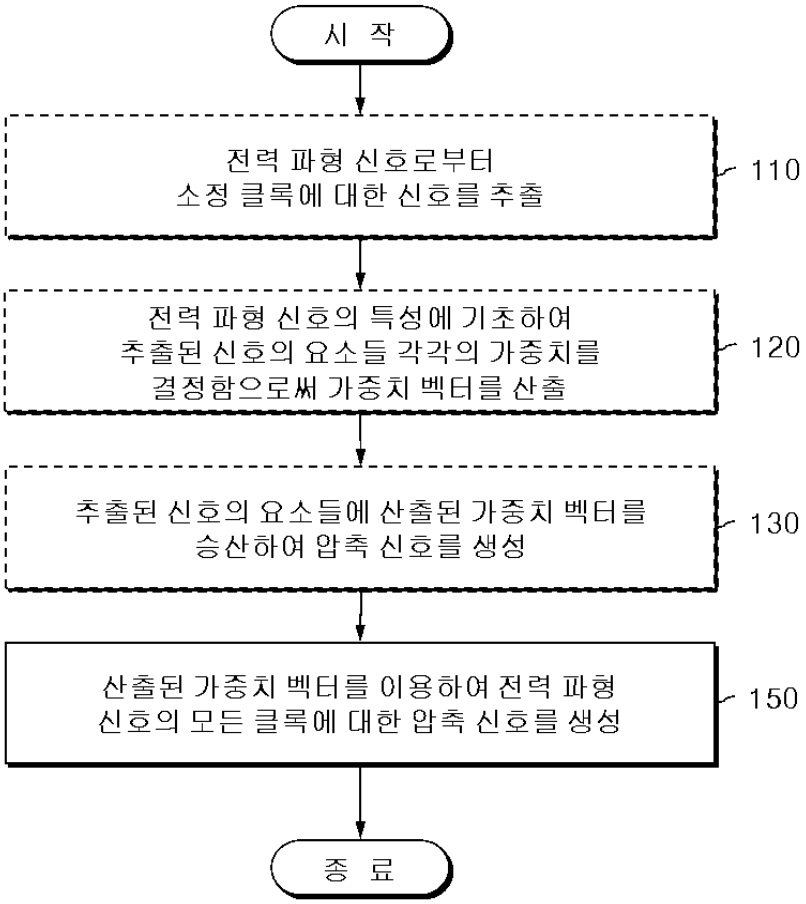
도면5b



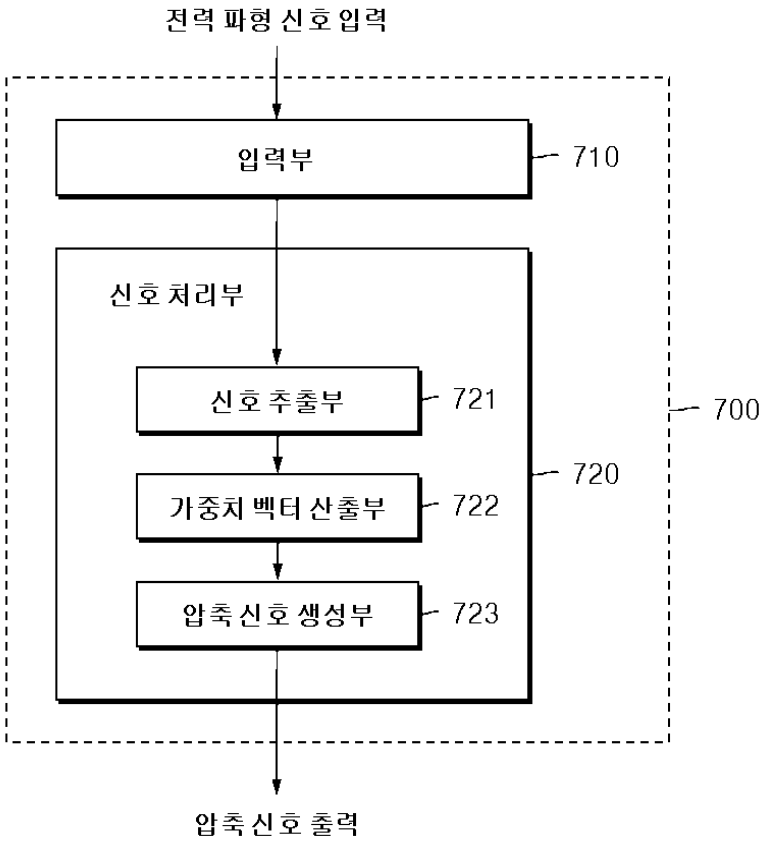
도면6a


시 작
전력 파형 신호로부터
소정 클록에 대한 신호를 추출
110
전력 파형 신호의 특성에 기초하여
추출된 신호의 요소들 각각의 가중치를
결정함으로써 가중치 벡터를 산출
120
추출된 신호의 요소들에 산출된 가중치 벡터를
승산하여 압축 신호를 생성
130
140
전력 파형
신호의 클록들
각각에 대해
반복하여 수행
종 료

도면6b


시 작
전력 파형 신호로부터
소정 클록에 대한 신호를 추출
110
전력 파형 신호의 특성에 기초하여
추출된 신호의 요소들 각각의 가중치를
결정함으로써 가중치 벡터를 산출
120
추출된 신호의 요소들에 산출된 가중치 벡터를
승산하여 압축 신호를 생성
130
산출된 가중치 벡터를 이용하여 전력 파형
신호의 모든 클록에 대한 압축 신호를 생성
150
종 료

도면7


전력 파형 신호 입력
입력부
710
신호 처리부
신호 추출부
721
가중치 벡터 산출부
722
압축 신호 생성부
723
720
700
압축 신호 출력